

NAVAL POSTGRADUATE SCHOOL
Monterey, California



THESIS

**A DISCRETIONARY-MANDATORY MODEL AS APPLIED
TO NETWORK CENTRIC WARFARE AND
INFORMATION OPERATIONS**

by

Daniel R. Hestad

March 2001

Thesis Co-Advisors:

James Bret Michael
Audun Josang

Approved for public release; distribution is unlimited.

20010328 054

REPORT DOCUMENTATION PAGE			Form Approved OMB No. 0704-0188	
Public reporting burden for this collection of information is estimated to average 1 hour per response, including the time for reviewing instruction, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing the collection of information. Send comments regarding this burden estimate or any other aspect of this collection of information, including suggestions for reducing this burden, to Washington headquarters Services, Directorate for Information Operations and Reports, 1215 Jefferson Davis Highway, Suite 1204, Arlington, VA 22202-4302, and to the Office of Management and Budget, Paperwork Reduction Project (0704-0188) Washington DC 20503.				
1. AGENCY USE ONLY (Leave blank)		2. REPORT DATE March 2001		3. REPORT TYPE AND DATES COVERED Master's Thesis
4. TITLE AND SUBTITLE : A Discretionary-Mandatory Model As Applied To Network Centric Warfare And Information Operations				5. FUNDING NUMBERS
6. AUTHOR(S) Hestad, Daniel R.				
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) Naval Postgraduate School Monterey, CA 93943-5000				8. PERFORMING ORGANIZATION REPORT NUMBER
9. SPONSORING / MONITORING AGENCY NAME(S) AND ADDRESS(ES) N/A				10. SPONSORING / MONITORING AGENCY REPORT NUMBER
11. SUPPLEMENTARY NOTES The views expressed in this thesis are those of the author and do not reflect the official policy or position of the Department of Defense or the U.S. Government.				
12a. DISTRIBUTION / AVAILABILITY STATEMENT Approved for public release; distribution is unlimited.				12b. DISTRIBUTION CODE
13. ABSTRACT (maximum 200 words) The concepts of DoD information operations and network centric warfare are still in their infancy. In order to develop these concepts, the right conceptual models need to be developed from which to design and implement these concepts. Information operations and network centric warfare are fundamentally based on trust decisions. However, the key to developing these concepts is to develop for DoD is to develop the organizational framework from which trust, inside and outside, of an organization may be achieved and used to its advantage. In this thesis, an organizational model is submitted for review to be applied to DoD information systems and operational organizations.				
14. SUBJECT TERMS Trust models, Network Centric Warfare, Computer Security, Information Operations				15. NUMBER OF PAGES 100
				16. PRICE CODE
17. SECURITY CLASSIFICATION OF REPORT Unclassified		18. SECURITY CLASSIFICATION OF THIS PAGE Unclassified		19. SECURITY CLASSIFICATION OF ABSTRACT Unclassified
				20. LIMITATION OF ABSTRACT UL

Approved for public release; distribution is unlimited

**A DISCRETIONARY-MANDATORY MODEL AS APPLIED TO NETWORK
CENTRIC WARFARE AND INFORMATION OPERATIONS**

Daniel R. Hestad
Lieutenant, United States Navy
B.S., University of Wisconsin, 1994

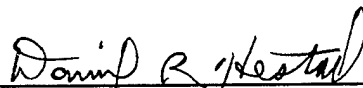
Submitted in partial fulfillment of the
requirements for the degree of

MASTER OF SCIENCE IN INFORMATION SYSTEMS AND OPERATIONS

from the

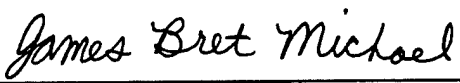
**NAVAL POSTGRADUATE SCHOOL
March 2001**

Author:



Daniel R. Hestad

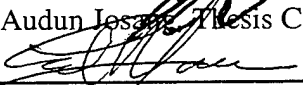
Approved by:



James Bret Michael, Thesis Co-Advisor



Audun Iosad, Thesis Co-Advisor



Carl R. Jones, Chairman
Information Systems and Operations
Curriculum Committee

ABSTRACT

The concepts of DoD information operations and network centric warfare are still in their infancy. In order to develop these concepts, the right conceptual models need to be developed from which to design and implement these concepts. Information operations and network centric warfare are fundamentally based on trust decisions. However, the key to developing these concepts is to develop for DoD is to develop the organizational framework from which trust, inside and outside, of an organization may be achieved and used to its advantage. In this thesis, an organizational model is submitted for review to be applied to DoD information systems and operational organizations.

TABLE OF CONTENTS

I. INTRODUCTION.....	1
A. INFORMATION TECHNOLOGY AND TRUST	1
B. INFORMATION INFRASTRUCTURE	2
C. INFORMATION SECURITY	3
1. INFORMATION ATTACK VULNERABILITIES	5
2. THE HACKER THREAT	7
3. TRUST IN SYSTEMS	9
D. PUBLIC KEY INFRASTRUCTURE.....	11
E. PROBLEMS WITH PUBLIC KEY CRYPTOGRAPHY.....	13
1. KEY MANAGEMENT ATTACKS.....	14
2. TOTAL SYSTEM COLLAPSE	14
3. SECURITY OF CERTIFICATES	14
F. RESEARCH QUESTIONS	15
G. LITERATURE REVIEW	15
1. INFORMATION SECURITY	15
2. TRUST MODELS	16
3. INFORMATION OPERATIONS	16
H. EXPECTED BENEFITS OF THESIS.....	17
I. ORGANIZATION OF THESIS.....	17
II. WHY IS TRUST IMPORTANT?.....	19
A. WHAT IS TRUST?.....	19
B. ORGANIZATIONAL TRUST THEORY	20
C. THE COST OF DISTRUST	22
D. TRUST AND PUBLIC KEY INFRASTRUCTURE	23
E. TRANSITIVITY OF TRUST	24
F. TRUST AND OPEN SYSTEMS.....	24
G. MOBILE AND DISTRIBUTED SYSTEMS	25
H. TRUST MANAGEMENT.....	26
III. TRUST AND INFORMATION OPERATIONS	29
A. INFORMATION OPERATIONS.....	29
B. RISK MANAGEMENT/UNCERTAINTY	30
C. THEATER ENGAGEMENT PLAN	33
D. PERCEPTION MANAGEMENT	37
E. DECEPTION	38
F. THE ECONOMY	39
G. PKI AND INFORMATION OPERATIONS.....	40
H. PKI IN THE WRONG HANDS/COMPROMISE.....	41
IV. THE DISCRETIONARY-MANDATORY MODEL	43
A. INDUSTRIAL AGE	43
B. DISTRIBUTED MODEL	44
C. INFORMATION AGE	45
D. DISCRETIONARY-MANDATORY MODEL	46
E. MANDATORY POLICIES	47
F. DISCRETIONARY POLICIES	48
G. RULES AND PRECEDENCE.....	49
H. INCORPORATING TRUST INTO THE D-M MODEL	50
I. RECIPROCAL TRUST	53
V. CASE STUDY – BATTLEFIELD INFORMATION DISSEMINATION.....	55

A. DEFENSE INFORMATION INFRASTRUCTURE	55
B. COMMAND AND CONTROL.....	57
C. TACTICAL INFORMATION PROCESSING.....	57
D. CASE STUDY – BATTLE GROUP CONNECTIVITY	59
1. INFORMATION OPERATIONS	62
2. THEATER ENGAGEMENT PLAN.....	63
E. HUMAN FACTORS	64
F. INCORPORATION OF THE D-M MODEL	64
VI. CONCLUSION	67
A. SUMMARY.....	67
B. THE D-M MODEL.....	68
C. TRUST RELATIONSHIPS	68
D. TRUST IN THE ORGANIZATIONAL ENVIRONMENT	69
E. INFORMATION OPERATIONS AND NETWORK CENTRIC WARFARE	70
F. FUTURE WORK.....	71
1. IMPLEMENTATION OF THE D-M MODEL INTO U.S. DOD INFORMATION SYSTEMS	71
2. A WORKING D-M TRUST MODEL.....	71
3. QUANTIFYING THE HUMAN FACTORS OF THE D-M MODEL.....	72
4. DEVELOPING A PROTOTYPE OF THE D-M MODEL	72
5. APPLY THE D-M MODEL TO U.S. DOD INFORMATION SYSTEMS	73
6. APPLY THE D-M MODEL TO A NETWORK CENTRIC WARFARE ORGANIZATION.....	73
7. ANALYZE THE MODEL WITH SOFTWARE.....	74
LIST OF REFERENCES.....	75
APPENDIX. GLOSSARY.....	79
INITIAL DISTRIBUTION LIST	83

LIST OF FIGURES

FIGURE 1. INFORMATION INFRASTRUCTURE (FROM JOINT PUBLICATION 3-13)	3
FIGURE 2. PUBLIC KEY INFRASTRUCTURE.....	12
FIGURE 3. INFORMATION OPERATIONS AS A STRATEGY	29
FIGURE 4. THEATER ENGAGEMENT PLAN (STEINKE & TARBET, 2000)	36
FIGURE 5. IO IN THE SPECTRUM OF CONFLICT	38
FIGURE 6. TOP-DOWN HIERARCHY	43
FIGURE 7. DISTRIBUTED ARCHITECTURE.....	45
FIGURE 8. THE DISCRETIONARY-MANDATORY MODEL.....	47
FIGURE 9. TRUST MATRIX.....	51
FIGURE 10. INFORMATION INFRASTRUCTURE.....	55
FIGURE 11. TACTICAL INFORMATION PROCESSING.....	58

ACKNOWLEDGMENT

The author would like to sincerely thank Bret Michael and Audun Josang whose guidance and wisdom throughout the entire process was unyielding and admirable. Thanks also to my wife, Lori, who endured countless books being thrown against the wall in frustration.

I. INTRODUCTION

Mankind has had an agrarian existence for at least ten thousand years. Christianity is almost two thousand years old. The New World was "discovered" a little over five hundred years ago. Industrial development started approximately two hundred years ago. The age of the Internet, with the development of the World Wide Web, is five years old (Power, 1999).

A. INFORMATION TECHNOLOGY AND TRUST

With the explosion of information technology over the past decade and the rapid move from an industrial-based economy to one which is information based, the concepts of Network Centric Warfare and Information Operations (IO) have become increasingly integrated to our national strategy and the conduct of military operations. In practice, however, these concepts remain very loosely defined.

Information technology has created a world where huge amounts of data can be transported nearly instantaneously. While this has spawned many new corporations and fortunes, it has presented many problems. Security, privacy, authenticity, integrity are all issues associated with the new economy.

How does an individual verify the identity of another entity over a network? Further, how does one verify the quality and integrity of the data he receives over the same network? These problems are somewhat trivial in the cases of an Internet chat room, or e-mail. They may cause some embarrassment if the real identity is revealed, or a widespread nuisance in the case of an e-mail virus.

But what if a corporation is negotiating with another corporation? If the data to be exchanged is stolen, corrupted, altered, or tampered with, huge amounts of money may be lost. In planning a military operation, the lives of many people may depend on the integrity of key information.

Technology has presented us with these problems, but it also offers a solution. The Public Key Infrastructure (PKI) was designed to solve key management problems. However, it has created trust management problems.

Trust in any system is paramount to the proper function of the system. We take our money to a bank because trust it will be there when we want to withdraw it. We travel on airplanes because we trust the airlines to transport us from Point A to Point B safely and in a reasonable amount of time. We report suspicious behavior to the proper law enforcement officials because we trust they will investigate and take the correct action. We trust these systems as well as many others. Sometimes our trust is misplaced but there are mechanisms in place to correct the system when the system is deemed untrustworthy.

B. INFORMATION INFRASTRUCTURE

There are several domains in which the United States exchanges and stores its information. Joint doctrine recognizes three: the Global Information Infrastructure (GII), the U.S. National Information Infrastructure (NII), and the Defense Information Infrastructure (DII).

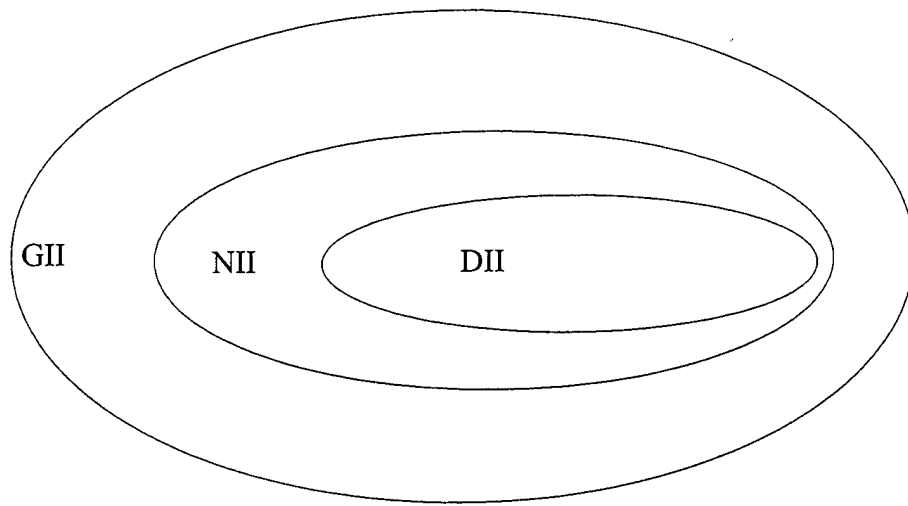


Figure 1. Information Infrastructure (From Joint Publication 3-13)

Each infrastructure maintains its own characteristic system of interconnected computers, communications networks, databases, sensors, software, operators, and other elements which serve the information processing demands of the users within the Department of Defense, United States Government, and the entire world.

C. INFORMATION SECURITY

In the computing evolution from standalone and mainframe computers to networks of personal computer workstations, systems have become more vulnerable to attack. User trust in the Internet has eroded as reports of vulnerabilities (e.g., bugs) and threats (e.g., hacker exploits) appear in the news. As the Internet continues to expand,

uncertainty and risk of compromising confidential information from hostile or careless users also expands. (Gaines, 2000)

The Web has rapidly evolved from its original purpose as a research tool (ARPANET) to a worldwide forum for conducting diverse electronic transactions. Industry, government, and private citizens have become dependent on the global communication channels provided by the Internet. Worldwide connectivity has brought us closer to becoming the “global village” envisioned by some, while also introducing both threats and vulnerabilities. (Friedman, 1999)

Modern, high-speed, networked systems have created a number of new threats and vulnerabilities. Networks are vulnerable to attack from multiple areas and from a long distance. Attacks can arise from inside the network or externally through the Internet. If a machine is connected to an external network, physical security is only part of the security equation. The same paths which allow remote access also afford access paths to attackers.

The expansion of remote login capability has also introduced additional vulnerabilities. Usually, a modem would offer one service, the ability to login. The ability to send mail and perform other tasks was channeled through this single choke point. With the advent of networking, multiple services were offered such as FTP, login, disk access, remote execution, and system status. These services add to the number of things that must be addressed when protecting computer assets. (Chestwick, B. and Bellovin, S., 1994)

Networked systems also integrate numerous computer components and communication systems. A network is only as secure as the most vulnerable component on the network. Organizations purchase software and hardware from commercial vendors, so they have little or no influence on the design of the COTS component and may not possess any detailed information on the internal workings of those components. Hence, users may have to rely on the trustworthiness and claims of the manufacturers as to the security of these components. Additionally, it is difficult to predict or know what can and cannot happen within any complex system and what can be done to control the behavior of that system (National Research Council, 1999).

Modern networks present several security problems. In order to establish trust in such a computing environment, the public must be convinced that the threats associated with vulnerabilities can be controlled or prevented. Unfortunately, security vulnerabilities are difficult to identify until they have been breached. Moreover they cannot be controlled.

1. Information Attack Vulnerabilities

Virus attacks have increased the risk associated with being connected to the Internet and as a result they have contributed to distrust of the Internet. A virus is a piece of software which self-replicates from host to host. A virus can be malicious code embedded in an executable program that will perform undesirable tasks such as deleting files, interfering with memories and slowing down processing speeds. Viruses used to be spread through infected floppy disks, however, today they tend to be attached to e-mail,

downloadable programs, and mobile code. The first two known major malicious virus attacks occurred in late 1987. (Kabay, M., 1996) This attack was spread through a university computer lab via infected floppy disks.

Reportedly, there are about 46,000 different viruses. The costs of a virus attack vary, although an USA Research study reported costs at \$800 per PC infected. (Kabay, M., 1996) Large attacks have resulted in costs of over one million dollars. Although the use of anti-virus software is more prevalent than ever before, those creating viruses are also becoming more sophisticated.

People must exercise caution when downloading programs from untrusted sources. Sometimes programs advertised as shareware or freeware may contain a Trojan horse. A Trojan horse is an apparently useful and innocent looking program that has undetectable malicious functions. An example is a computer-based game that when installed also copies private files and e-mails them to another site. Common trojan horse programs are detectable by antiviral software, but some, like the new Back Orifice program contain polymorphic stealth technology and are difficult to detect.

A back door is an unauthorized and undocumented path for accessing information. Sometimes a programmer will intentionally install a back door for maintenance purposes, or it can be an undocumented feature of the program that allows a rogue user special privileges. Back doors are usually inserted via Trojan horse programs, but they have also been found in commercially provided software packages as well. (Gaines, 2000) Robert Morris utilized a back door in the debug option for the sendmail program in the UNIX

system to launch his worm attack. They can be installed in software during manufacturing or distribution. Trap doors are very difficult to detect. (Kabay, M., 1996)

The topologies and protocols which make it possible for networks to communicate with each other also makes them vulnerable to packet sniffing. When a packet is sent on an Ethernet or Token Ring local area network (LANs), all of the computers on that LAN will receive the message. Then each computer will read the packet header information to determine the destination address. If the destination address agrees with their machine address, they accept the packet; otherwise they discard the packets. A sniffer is a device that monitors the traffic along the LAN and instead of discarding packets; it captures and copies them. By putting a network interface card (NIC) card in promiscuous mode, all traffic along the LAN can be read. This vulnerability is used by hackers to gain information on passwords, credit cards, and other private information. (Comer, 1999)

2. The Hacker Threat

Hackers are people who exploit information systems either for their own amusement or to commit criminal acts. Hackers are able to access systems by using the pathways provided by the Internet to utilize those flaws in software and operating systems. Many companies will not report penetrations of their security systems, so it is difficult to measure the damage inflicted by hackers. They fear that exposure of security incidents will undermine public confidence in their computing systems and the safeguard of the funds and private information.

Hackers have gained a great deal of notoriety in the press and in movies. "WarGames", "Whiz Kids", and The Cuckoo's Egg, are notable examples. Hackers are portrayed as resourceful, clever, gifted, but misunderstood individuals. Many hackers themselves defend their actions by saying they perform a service by exposing security flaws. This may, in fact, be true. But, hackers also directly contribute to the public's distrust of the computer as a secure mechanism for facilitating information flow. Hackers have exposed the public to the realization that there are security vulnerabilities in the Internet and computing systems. (Gaines, 2000)

A common misconception is that hackers are ingenious programmers. There are a few hackers who fall into this category. But the vast majority are using downloadable software, designed by other people, and easily obtained through the Internet. Step-by-step instructions on how to use these programs are often available. One particularly attractive hacker website, www.inforwar.co.uk/articles/simpnt4.htm, Lopht crack (a program for cracking passwords), getadmin and crack4.exe (used to insert a user account into the password file) are readily available for download. Back Orifice 2000 can be downloaded from the Cult of the Dead Cow homepage. (Gaines, 2000)

The widespread reports of computer hacking have seriously damaged the trust we have in any computer network. As soon as a new product is released - whether it be software or hardware - a litany of security vulnerabilities and available patches is sure to follow. Computer security is a battle which is fought every day and must be managed and weighed against cost and other factors. Unless a machine is completely isolated from all other systems, and therefore virtually useless, it will be vulnerable to attack.

3. Trust in Systems

While the Internet is an untrustworthy entity, there are mechanisms that an organization can install that will ensure a measure of trust in that organization. (Gaines, 2000) Computer security is typically described in terms of confidentiality, authentication, nonrepudiation, integrity, and availability. Confidentiality means that private information is accessible only to those authorized to access it. Authentication identifies the actual sender of a message. Nonrepudiation means a user cannot disavow himself from an action he has already taken. Integrity means that the message itself has not been modified. Availability ensures that the network and the information contained in the network are accessible when needed. No single security mechanism can provide complete security, but by combining different security mechanisms we can provide a reasonable level of trust in the system.

Authentication is usually done by challenging a user with something he knows, something he has, or something he is. A common authentication is the password, which is something the user knows. Personal identification numbers (PINs) are another example. Identification or smart cards, badges, are examples of something the user has. Authentication procedures will typically combine something a person has with an object he possesses, such as an ATM card with a PIN number, or a username and password. Biometric devices such as eye scanners, fingerprints, and voice authentications, make use of a person's unique physical characteristics.

Digital signatures are used to verify the integrity of information. They are formed by combining a public key algorithm with a hashed algorithm. The original message is

run through the hash algorithm. The hash value is attached to the message and to the recipient. The recipient verifies the hash by putting the message through the same hash algorithm again. If the message has been modified in transit, the hash values will not match. The hash value itself is encrypted with the sender's private key. The receiver verifies the hash by decrypting it with the sender's public key. A digital signature provides authenticity as well as non-repudiation, because the private key identifies the sender. In the United States, digital signatures are now recognized by law as legitimate forms of proof of signature for legal transactions.

Availability is dependent on a number of factors. Network configuration, bandwidth, user training, security, weather, just to name a few. An official from the Computer Emergency Response Team (CERT) stated that most organizations regard availability as the most important quality of a system. (Schimmel, 2000) In order to help maintain availability, firewalls can be installed to prevent unwanted packets from entering the system and disrupting service (i.e. a message flood, denial of service attack). Intrusion detection systems can alert network managers when an unauthorized user is exploring the system. These measures have costs associated with them. A tight firewall also degrades system performance. Intrusion detection systems are reactionary and only notify us that someone is or was in the network.

"The degree to which a system can provide authenticity, integrity, confidentiality, and availability determines the level of risk associated with that system. The extent to which a system is secure helps establish the level of trust afforded to a system." (Gaines, 2000) Unfortunately, it is extremely difficult to judge a system's security posture unless

one is intimately familiar with it, or it has been evaluated by a reputable outside agency. The Internet is a “network of networks,” each with its own security postures, policies and thresholds. Thus, it is extremely difficult to evaluate trust among entities on the Internet.

In today’s world of electronic commerce, trust has become an important asset. An untrusted organization will probably not be able to do business and may eventually fail. Many transactions today, are not done face to face. They are done via desktop, networks, video-teleconference, and in some cases by intelligent agents. Money changes hands but this takes place via electronic funds transfer. Handshakes are quickly becoming a thing of the past. Traditional legal methods of paper contracts and signatures that legally bind entities to that contract are inadequate.

The security policies of an organization are important in determining its trustworthiness. But there are other factors. After verifying the integrity, confidentiality and authenticity of the data, how reliable is the person or people who provided you with the information. Public key certificates are useless if the person who owns the key is unreliable. If trust is to be injected into our basic communications systems to conduct day-to-day business, trust itself must be understood and effectively managed.

D. PUBLIC KEY INFRASTRUCTURE

Traditional cryptographic methods have been around for thousands of years. Julius Caesar used encryption methods to send important communications to his generals and his allies. The process was simple. To use conventional names, Alice would take a message, M . Encrypt M , using a key, K to get an encrypted message, M_K . She would

then send the encrypted message, M_K , to the intended receiver, Bob. The receiver would then decrypt M_K , using the same key, K . The result: the original plaintext message, M .

There are problems, however, with this system of symmetric encryption. Namely, how does the sender get the key safely to the intended receiver. This would usually necessitate some predetermined arrangement of which keys to use on a given day, or for a certain type of message. Also, there is no mechanism to authenticate the originator of the message, or that the contents of the message had not been altered en route to its destination. Additionally, if the message is intercepted, the strength of the encryption technique is called into question. A weak encryption technique means it is possible the message will be decrypted by the enemy and its contents compromised.

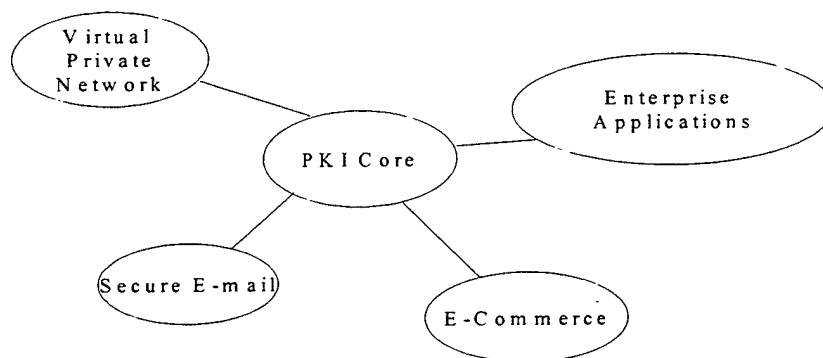


Figure 2. Public Key Infrastructure

Public key cryptographic methods solve each of these problems. The public key system uses two keys; one public and one private. The RSA algorithm, developed in

1977, allows a message to be encrypted with one key and decrypted with a different key. The Public Key Infrastructure (PKI) is based on this asymmetric type of encryption.

Assymmetric keying works as follows. Alice wants to send an encrypted message to Bob. She contacts a Certification Authority (CA) which maintains a database of public keys or certificates. The CA verifies Alice's identity and transmits her Bob's public key. She then encrypts the message using Bob's public key and transmits it to Bob. When Bob receives the message he decrypts it using his private key which he is responsible for, similar to an ID card. He then has the plaintext message.

If Alice had also wanted to provide a digital signature, she could do so by running the message through a hash function which provides a summary of the message. She then would encrypt this hash code with her private key and attach it to the end of her message. In order to verify that the message was indeed sent by Alice, Bob would simply use her public key to decrypt the code and apply the same hash function.

E. PROBLEMS WITH PUBLIC KEY CRYPTOGRAPHY

While public key encryption solves many classical problems associated with traditional encryption methods, it also brings with it some problems of its own. As new forms of encryption become available, new forms of attack will tend to follow. Consideration of several new forms of attack must be made before we envoke our trust in the system.

1. Key Management Attacks

Certificate Authorities (CA) carry an enormous responsibility in the PKI system and represent a single point of failure. If the security practices of the CA are breached, the confidence in those identities that are verified by that CA are called into question.

2. Total System Collapse

The RSA algorithm, upon which the public key system is based, relies on the difficulty of prime factoring extremely large numbers. For example, find the prime factors of 731. The answer would be 17 and 43. But the problem would be much more difficult if the number to factor was 400 digits in length. If any significant advances, however unlikely, occur in the field of mathematics, particularly computational number theory, the public key method could quickly become vulnerable. It would then be disastrous if our sole method for keeping data secure was based upon this algorithm.

3. Security of Certificates

Most practical implementations of PKI require a product termed a “smart card.” Similar in appearance to a credit card or a driver’s license, the “smart card” carries the necessary personal and PKI data to complete the authentication and digital signature process. Presumably, the card would be carried in one’s wallet or purse for easy accessibility. Several European countries have begun the use of prototype cards. In Finland, a card produced by International Data Group (IDG) is used to conduct secure electronic transactions nationwide. They call their cards electronic identification or EID cards.

But what are the mechanisms to prevent false cards from being produced? How is identity theft prevented? What if a card is lost? How does a CA revoke privileges once they have been granted?

F. RESEARCH QUESTIONS

The following questions will be addressed in this thesis:

1. What is the Discretionary-Mandatory (DM) trust model?
2. How does the D-M model apply to DoD systems?
3. What is trust?
4. How does trust apply to Information Operations?
5. What does trust mean to the military commander?
6. How does the D-M model facilitate trust inside an organization?
7. How does the D-M model facilitate trust between organizations?

G. LITERATURE REVIEW

1. Information Security

Information security is a multi-disciplinary occupation. Among the broad range of subjects are cryptography, computer science, and communications technology.

Cryptography is an age-old practice and as such is well-documented. A highly recommended source and most comprehensive reference is Bruce Schneier's book *Applied Cryptography*. (Schneier, B., 1996) There are many authors who discuss modern

computer security. This thesis will rely on textual material including *Computer Networks and Internets* by Douglas Comer, *Security in Computing* by Charles Pfleeger, and *Information Warfare and Security* by Dorothy Denning.

2. Trust Models

The subject of trust models is well-developed in the business world. However, it has rarely been applied to information technology and trusted electronic systems. *Trust In Organizations: Frontiers of Theory and Research*, a collaborative work by Roderick M. Kramer and Tom R. Tyler, describes a scientific approach to trust models in business organizations. For current research regarding trust models, this thesis will rely heavily on the work of Professor Alfarez Abdul-Rahman, University College London, and Professor Audon Josang, University of Queensland. They provide the most extensive and insightful research on the principles of trust and trust modeling.

3. Information Operations

Information Operations is still in its genesis phase, however, a great deal of literature already exists on the subject. Joint Publication 3-13 will be the primary source for formal DoD definitions. Several key authorities in various DoD and other governmental agencies will be consulted for their views and opinions as well. These agencies will include, but are not limited to, the National Security Agency (NSA), Defense Information Systems Agency (DISA), and the Computer Emergency Response Team (CERT).

H. EXPECTED BENEFITS OF THESIS

The concept of trust and trust modeling is taking root in the development of information systems and security. Many trust models have already been developed and submitted for integration into security systems. Unfortunately, many of these models reflect an either/or mentality. They either support a distributed architecture or a centrally controlled architecture. Further, they do not recognize trust as an organizational concept.

The Discretionary-Mandatory model, submitted for review is not a trust model. It is an organizational model, which, when applied supports flexibility and timely decision-making processes while also providing standardization across many different organizations.

I. ORGANIZATION OF THESIS

Chapter II will provide a scientific explanation of trust and trust models. Further, it will state the case of why trust is important in any system, but particularly a virtual system with no apparent means of authentication other than with digital encryption measures.

Chapter III will explain the definitions and concepts of Information Operations and explain why, in the age of globalization and information technology, the concept of trust is critical to the military's notion of Information Operations.

Chapter IV will present for review a new model which more accurately reflects trust decisions. Called the Discretionary-Mandatory (D-M) model, it will be based on the concept of some centrally enforced rules and some locally enforced rules.

Chapter V will describe a case study in which the D-M model will be applied in practice in a combat decision sequence. Chapter VI will consist of conclusions and recommendations for future research.

II. WHY IS TRUST IMPORTANT?

Dennis saw the hacker problem in terms of social morality. "We'll always find a few dodos poking around our data. I'm worried about how hackers poison the trust that's built our networks. After years of trying to hook together a bunch of computers, a few morons can spoil everything."

I didn't see how trust had anything to do with it. "Networks are little more than cables and wires," I said.

"And an interstate highway is just concrete, asphalt, and bridges?" Dennis replied. "You're seeing the crude physical apparatus-the wires and communications. The real work isn't laying wires, it's agreeing to link isolated communities together. It's figuring out who's going to pay for maintenance and improvements. It's forging alliances between groups that don't trust each other."

"Like the military and universities, huh?" I said, thinking of the Internet.

"Yes, and more." (Stolle, 1990)

A. WHAT IS TRUST?

Defining and quantifying trust is difficult. Gerck defines trust as "that which is essential to a communication channel but cannot be transferred from a source to a destination using that channel". (Gerck, 1998) This is somewhat abstract and difficult to conceptualize. A more common approach would be to compare information and trust; information is what you do not expect and trust is what you know and can verify. (Gerck, 1998) Information systems are built to transfer and store information. To clarify, if one receives a piece of data which is already known, he has not enhanced his concept of reality and has received no information. If, however, he receives data which was not known, he has value added and has received information.

Trust in a system is what allows a system to work. Without it nothing else matters. The banking system works because its users trust in the system. Most of us have never personally met the management of the institution with which we conduct our banking transactions, we do not review their balance sheets, we do not check the source code of their computer systems for errors, and we do not run background checks on bank employees. But we trust our bank with our money; at least most of it. Why? Because there are mechanisms in place, namely federal banking laws, which give us a measure of trust in the system, provide a system of accountability of the institution itself, and a social penalty for abuse of untrustworthy behavior.

Fundamentally, trust is a belief. This belief may be conditioned on personal knowledge, examination, individual qualifications, certificates from recognized and trusted authorities, negotiation, established commonalities, and experimentation over time. Beliefs are usually hard to establish, but easier to call into question or disestablish. Trust, once given – then broken, is most difficult to reestablish. It is the reestablishment that we must deal with in our information systems as the most problematic, that is trust management.

B. ORGANIZATIONAL TRUST THEORY

Social scientists have used a “rational choice” model for describing general social behavior and decision-making for the past few decades. This model is based upon the belief that people are, in general, compelled to maximize their personal gain and minimize their personal losses. This leads to a general inability to achieve cooperation in

many social environments, namely the business and professional environment. It also breaks down due to an inability of people to accurately assess their own self-interests. In the absence of formal trust and accountability mechanisms, both of these decision stimulæ account for a general lack of trust among even close associates. Tyler and Kramer state that, "People have, in fact, been found to have difficulty effectively building cooperation in negotiations with others." (Kramer & Tyler, 1996)

In recent years, this "rational choice" model has been questioned in its accuracy to describe our social behavior. Kramer describes a more accurate model as "social contextualism" because it views "individuals as fundamentally and essentially social decision makers." (Kramer 1994) How is trust perceived in a model of social contextualism? According to Kramer and Tyler,

American society is moving away from supporting long-term social connections between individuals and between individuals and organizations. In the family arena, the emergence of no-fault divorce discourages long-term interpersonal commitments. In work, the development of the "contingent workforce" discourages loyalty to work organizations. In this evolving world, people increasingly cannot count on loyalty to others as a basis for reciprocity. They cannot trust others. A wife, for example, cannot point out to her husband that she abandoned her career to raise their family and expect to invoke an obligation that will be honored, just as workers cannot loyally support their organization over the years and expect that organization to place a high priority on their pension needs. In a world without such reciprocal obligations, it is hardly surprising that people are interested in learning how to negotiate effectively to protect their self-interests. (Kramer & Tyler, 1996)

Organizational structures are changing. The speed at which information and data moves today is forcing changes to be made in traditional hierarchial and bureaucratic organizations; these organizations are disappearing and being replaced by lateral alliances and social relations. This necessitates more freedom of action by the individual which, in turn, creates a need for mechanisms to apply trust to information systems.

C. THE COST OF DISTRUST

Trust can be considered an asset for an organization. It has a cost, but that cost diminishes over time as the organization maintains trusted relationships with other organizations. "It is the expectation of an ongoing relationship that sustains trust in the actions of others. (Kramer & Tyler, 1996) For example, a startup company relies on several new employees at all levels of management. Presumably, these employees have never met each other and have no established relationship. It will take time to develop trust among fellow workers and until trust is developed, production time will lag, *ceteris paribus*. But once trust is cultivated and developed in the organization, tasks will be completed much sooner, production time will quicken and costs will decrease. Cultivating trust in an organization should be a major goal of management.

Additionally, the same company will want to develop business relationships with other companies. Initially, the trust factor will be low. The possibility of failure on another company's part will have to be accounted for in the company's operational plans. However, as business and interpersonal relationships develop, management will have a better understanding of what companies they can trust to meet their commitments and

what companies they cannot trust. More accurate plans can be developed, coordination can be more tightly synchronized, and both fixed and variable costs will fall.

Conversely, if an organization does not cultivate trusted relationships, inside and outside of the organization, the lack of trust will result in increased cost because management will continually be forced to re-evaluate relationships and account for the possibility of untrustworthy behavior.

D. TRUST AND PUBLIC KEY INFRASTRUCTURE

PKI is a means to develop and exchange credentials (keys) that validate the authenticity of each party and establish a trusted common session to perform an action. "Trust, as a subjective assessment made whenever information is used, is influenced by a variety of factors which vary based upon the person making the trust assessment." (Hansen, 1999) "Common factors that affect trust include privacy, operational necessity, risk assessment, and security services provided. Public key infrastructures are said to support or transfer trust because they facilitate the provision of security and/or privacy services with an established level of assurance." (Hansen, 1999) Simply validating the identity of a user does not necessarily infer trust. An individual is still free to question the legitimacy and accuracy of information coming from another user, even after his identity has been verified. There is still an element of risk and risk management involved in the transaction. As secure as the RSA algorithm might be, it still cannot counter the adage, "garbage in, garbage out."

E. TRANSITIVITY OF TRUST

There is a common assumption when describing trusted systems: the assumption that trust is somehow transitive. For example, if Alice trusts Bob, and Bob trusts Cathy, then Alice should and will trust Cathy. Trust is transitive under certain conditions.

Abdul-Rahman & Hailes propose the four conditions under which trust may be transferred:

- a) Bob explicitly communicates his trust in Cathy to Alice, as a 'recommendation'
- b) Alice trusts Bob as a recommender, that is, recommender trust exists in the system
- c) Alice is allowed to make judgements about the 'quality' of Bob's recommendation (based on Alice's policies)
- d) Trust is not absolute, that is, Alice may trust Cathy less than Bob does, based on Bob's recommendation

Abdul-Rahman and Hailes term this situation *conditional transitivity*.

F. TRUST AND OPEN SYSTEMS

An enormous problem which affects the internet as well as mobile networks and distributed databases is the openness of the systems. Tracking users globally, logging their activity, while at the same time providing quality service is simply infeasible. Markets and consumers are constantly demanding higher data rates, global access and less down time. At the same time, security and trust suffer. In reference to the three measures of information systems services - confidentiality, integrity and availability - an official

with the Computer Emergency Response Team (CERT) remarked, "more companies are demanding availability first, and care significantly less about confidentiality and integrity." Companies simply want access to their data, their e-commerce markets, their customers; if the data is bad, they will fix it later.

Since trust is difficult to transfer from one entity to another, a strictly authoritarian, centrally controlled system will have difficulty developing any degree of trust in this system. Not everyone trusts the same certificate authorities. Will foreign entities trust CA's from the United States or vice versa? No standards of trust for global PKIs have been addressed. Will military PKIs accept commercial certificates? Will universities accept military certificates? "Fixed architectures will probably not be reasonable in the sort of open environment like the internet; something more flexible and more adaptive is required." (Abdul-Rahman, 1996)

G. MOBILE AND DISTRIBUTED SYSTEMS

There is a trend in computing systems toward highly mobile, wireless and distributed systems. Laptops have been around for a number of years. Wireless LAN's have recently become a valued commodity. Palm pilots have been popular for the last few years. Automobile manufacturers are predicting the near availability of Internet devices in cars. The computing power of these devices compared to their size is enormous. With a device the size of a pocket calculator, a user can send e-mail, trade stocks, book an airline flight, etc. The security impact of these types of devices is significant. Wireless LAN's depend on radio frequency links. These links are then vulnerable to interception.

The reliance on centralized, distributed databases has also grown in recent years. How reliable are these databases? How are they populated? Who has access to them? Who has write access?

Data mining is the practice of gleaning computer systems for bits of data regarding an individual to piece together a profile to more effectively target that individual, usually for business marketing research and evaluation. Some people regard this as standard business practice, but others call it an invasion of privacy. Given the ease at which personal information is available, identity theft is a potential problem.

H. TRUST MANAGEMENT

In the physical world of human interaction, we trust people based on human factors. Appearance, reputation, and past social interactions all contribute to the degree of trust we place in another person. This is possible because the total number of people we have to trust is constrained by time and distance. (Josang & Tran, 2000) We do not require a Pentium III processor and a 40-gigabyte hard drive to keep track of human trust factors. By contrast, in the virtual world, time and distance are not factors. When we are online we have to trust people we do not even see; we may not know that they are even there. We have to trust the entire population of people online at the same time, because if we are all online, then we are all connected.

Josang and Tran define trust management as, “the activity of collecting, codifying, analyzing and presenting security relevant evidence with the purpose of making assessments and decisions regarding e-commerce transactions.” (Josang & Tran, 2000)

They also identify two basic approaches to trust management: policy-based management and subjective management. (Josang & Tran, 2000)

In a policy-based system, the extent to which an individual or organization relies on the binding between a certificate and its owner would depend on several factors, including the verification procedures of the CA to identify the true identity of a certificate holder, the CA's security procedures, its operating policy, storage facilities, etc. The policy-based approach is a useful from a management perspective because it specifies a set of objective evidence which is quantifiable and verifiable. (Josang & Tran, 2000) It would, however, require human inspection which takes time, in a world where automation is preferable.

A second approach, subjective trust management, would include subjective measures of trust inside the certificate. Credit ratings, background checks, and trust metrics could be combined within the policy and transferred in parallel from CA to CA. For example, within a certificate, it could be specified how much one CA trusts another CA. (Josang & Tran, 2000) This approach presents certain problems. In the PKI system, a CA should be the most trusted link in the chain. If CA's are not all trusted equally, it dilutes the overall trust in the system. Also, one CA might not want to advertise its distrust for another CA.

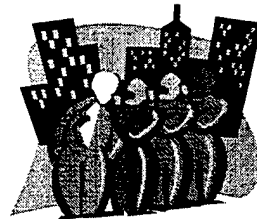
THIS PAGE INTENTIONALLY LEFT BLANK

III. TRUST AND INFORMATION OPERATIONS

A. INFORMATION OPERATIONS

Joint doctrine defines information operations (IO) as “actions taken to affect adversary information and information systems while defending one’s own information and information systems.” (Joint Pub 3-13) These actions apply across all phases of an operation from pre-hostilities to withdrawal and at every level of war. More specifically, Joint doctrine defines a set of IO capabilities, including, but not limited to, operations security (OPSEC), military deception (MILDEC), psychological operations (PSYOP), electronic warfare (EW), physical attack/destruction, and special information operations (SIO), which may include computer network attack.

INFORMATION OPERATIONS AS A STRATEGY



Information Operations Integrate Various Capabilities and Activities to Achieve National Military Objectives

Figure 3. Information Operations as a strategy

This definition, however, only speaks to the science of IO and its capabilities. The art of IO involves integrating these capabilities and achieving the desired effects on the

adversary. As illustrated in the figure above, extracted from Joint Publication 3-13, the "Joint Publication for Information Operations," IO is defined as a strategy for integration.

Since the Gulf War, the Department of Defense has attempted to articulate the real meaning of IO. JP 3-13 identifies the human decision making processes as the "ultimate target" for offensive IO. It is logical then that trust, an integral part of the human decision making process, is an important concept in its relationship to IO. As such, those involved with planning IO need to develop an understanding of trust and trust models and mechanisms for creating and maintaining trust in an information system.

B. RISK MANAGEMENT/UNCERTAINTY

The protected information environment is rooted in a sound approach to risk management. Risk management involves anticipating the needs in all defensive IO and includes planning for both protection and response based on a consideration of the information needs, value of the information which may be compromised or lost if the protected information environment is breached, information systems vulnerabilities, threats posed by potential adversaries, and those resources available for the protection and defense of the information environment. The value of information most likely will change from one phase of an operation to the next; risk management involve consideration of this this too. (Joint Publication 3-13)

In his most recent book, Bruce Schneier illustrates the genesis of how he has come to understand modern computer security. "I came to security from cryptography, and framed the problem with classical cryptography thinking. Most writings about security

come from this perspective, and it can be summed up pretty easily: Security threats are to be avoided using preventive countermeasures.” (Schneier, 2000) He goes on to write, “For decades we have used this approach to computer security. We draw boxes around the different players and lines between them. We define different attackers -- eavesdroppers, impersonators, thieves -- and their capabilities. We use preventive countermeasures like encryption and access control to avoid different threats. If we In his most recent book, Bruce Schneier illustrates the genesis of how he has come to understand modern computer security. “I came to security from cryptography, and framed the problem with classical cryptography thinking. Most writings about security come from this perspective, and it can be summed up pretty easily: Security threats are to be avoided using preventive countermeasures.” (Schneier, 2000) He goes on to write, “For decades we have used this approach to computer security. We draw boxes around the different players and lines between them. We define different attackers --eavesdroppers, impersonators, thieves -- and their capabilities. We use preventive can avoid the threats, we've won. If we can't, we've lost.” (Schneier, 2000) He explains his modern vision of computer security: “I had my epiphany in April 1999: that security was about *risk management*, that detection and response were just as important as prevention, and that reducing the "window of exposure" for an enterprise is security's real purpose.” (Schneier, 2000)

In decision making under uncertainty, the decision maker does not know the probabilities of the various outcomes. For example, the probability that a Republican will be president of the United States twenty-five years from now is not known. Sometimes

accurate prediction of a state of nature cannot be made. In these cases, the following criteria can be used to make decisions:

- Maximax (Maximizes the maximum outcome)
- Maximin (Maximizes the minimum outcome)
- Equally likely
- Criterion of realism (Weighted average)
- Minimax (Minimizes the maximum loss)

Decision making under risk is a probabilistic decision situation. Several possible states of nature may occur, each with a given probability. Given a decision matrix with conditional values and probability assessments, it is possible to determine the expected monetary value (EMV) for each alternative. The EMV is the sum of possible payoffs, weighted by the probability of that payoff occurring.

EMV (alternative I) = (payoff of first state of nature)

X (probability of first state of nature)

+ (payoff off second state of nature)

X (probability of second state of nature)

+ ... + (payoff of last state of nature)

X (probability of last state of nature)

(Render & Stair, 2000)

It is possible, within a margin of error, to analyze the risk to a particular communications system. It is then the correct application of risk management principles which will minimize the risk of compromised data transmissions.

C. THEATER ENGAGEMENT PLAN

"Engagement, while not yet widely embraced as a characterization of our basic global posture, seems to me to express quite well what we need to be about in the post-Cold War era, that we need to be engaged in the world, and that we need to be engaged with other nations in building and maintaining a stable international security system." (Skelton, 1993)

For most of the 1990s and into the 21st century, international "engagement" has been and will be the defining term in America's national security and foreign policy strategies. This approach has resulted in an enormous increase in the rate and scope of US military deployments. On any given day, for example, the US Army has more than 30,000 soldiers deployed in over 70 nations, not including those soldiers routinely stationed outside the United States. To manage this change and the military's implementation of the engagement strategy, the US Department of Defense has within the past two years required the regional Combatant Commanders to develop Theater Engagement Plans (TEPs) and report those plans to the Secretary of Defense. (Steinke & Tarbet, 2000) The primary purpose of these plans, according to Chairman of the Joint Chiefs of Staff (CJCS) Manual 3113.01, is "to develop a process to globally integrate military engagement activities." (CJCS Manual 3113.01)

Since the 1986 Goldwater-Nichols Act, the President has been required to develop and present to the Congress a National Security Strategy, discussing at the very least the vital global interests and objectives of the United States. The general strategies found in this document have evolved from the 1987 and 1988 Cold War versions, which emphasized the military as an instrument of power in the containment policy, through the 1990 to 1993 Bush Administration documents focusing on "collective engagement," to the Clinton Administration's "engagement and enlargement" strategies. President Clinton's 1995 National Security Strategy highlighted the policy for engagement, stating, "While the Cold War threats have diminished, our nation can never again isolate itself from global developments." (Clinton, 1995) Engagement has then become the defining term for US foreign policy as we enter the 21st century.

In order to emphasize its ongoing engagement activities and to "operationalize" engagement, the DoD requires the regional CINCs to publish their TEP's annually. CJCS Manual 3113.01 defines engagement as "all military activities involving other nations intended to shape the security environment in peacetime." (CJCS Manual 3113.01, 1998) These TEP's were initiated to develop a process to globally integrate military engagement activities. Why is the DoD concerned about "globally integrating" military engagement activities? This answer is not clear in the manual, but one assumes the answer is found in both political and fiscal issues. The Department of Defense has been working in a resource-constrained environment for most of the 1990s, and global policy integration provides a more efficient use of those scarce resources. Further, global integration allows

for a more coherent political application of the National Security Strategy, rather than five or six different interpretations and applications of that strategy. (Steinke & Tarbet, 2000)

The TEP requires each Combatant Commander to establish a Strategic Concept for his area of responsibility covering the next five years. Each CINC's Strategic Concept and the resultant plan are based upon the Prioritized Regional Objectives as listed in the Joint Strategic Capabilities Plan. While these plans are to be reviewed by the Joint Staff, the Office of the Secretary of Defense, the services, and others, each CINC retains final approval authority for his plan. Once the approved plans are submitted to the Joint Staff, they are bundled into a "family of plans" by the Joint Doctrine Division. Ultimately, they are provided to the CJCS and DOD for review and approved by the Chairman, JCS, as a family of plans. (Steinke & Tarbet, 2000)

Theater Engagement Planning Process	
Stage 1	
Phase I	Initiation
	CJCS/CINCs receive planning guidance from Secretary of Defense in Contingency Planning Guidance.
	CINCs receive planning guidance from CJCS in the Joint Strategic Capabilities Plan.
Phase II	Strategic Concept Development
	CINCs' prioritized theater, regional, and country objectives are derived.
	Strategic concept is developed.
	Resources required to execute the strategy are identified at macro level.
	Strategic concepts are reviewed and integrated, then collectively approved by CJCS.
	<i>The product is a completed strategic concept.</i>

Stage 2	
Phase III	<i>Activity Annex Development</i>
	Specific engagement activities are identified.
	Force and resource requirements are identified at the macro level.
	Force and resource requirements are analyzed.
	Shortfalls are identified.
	TEPs are completed.
	<i>The product is a completed Theater Engagement Plan.</i>
Phase IV	<i>Plan Review</i>
	TEPs are reviewed by the Joint Staff, services, supporting CINCs, and the Office of the Undersecretary of Defense for Policy.
	TEPs are integrated into a "family of plans."
	"Family of plans" is approved by the CJCS.
	TEPs are forwarded as a "family of plans" for review by the Office of the Undersecretary of Defense for Policy.
Phase V	<i>Supporting Plans</i>
	Supporting plans are prepared as required.
Figure 1. The Theater Engagement Planning Process.	

Figure 4. Theater Engagement Plan (Steinke & Tarbet, 2000)

The TEP should be the document from which IO in the theater is based. From the guidelines of the TEP should come the information campaign which leads to a positively perceived image of the United States by the object country.

Fundamentally, the TEP is based on trust. That is, trust between countries. We are trying to create a trusted environment in which a country's leadership believes the United States will act in the best interests of not only ourselves, but that country as well. That trust may be based upon years of cooperation, such as the United States' relationship with the United Kingdom (UK), or it may be more pragmatic, such as the United States' relationship with Russia. Generally, the UK trusts the US because the UK has a history of trusting the US and the US has a history of being trustworthy. Russia is forced to trust the US to some extent, because it is in Russia's best interest to trust the US; Russia needs economic support if it is to survive.

D. PERCEPTION MANAGEMENT

Perception management is defined in Joint Pub 3-13 as, "Actions to convey and/or deny selected information and indicators to foreign audiences to influence their emotions, motives, and objective reasoning; and to intelligence systems and leaders at all levels to influence official estimates, ultimately resulting in foreign behaviors and official actions favorable to the originator's objectives. In various ways, perception management combines truth projection, operations security, cover and deception and psychological operations."

Intelligence preparation of the battlespace (IPB) is the process by which a database of potential operating areas is built. Perception management can be thought of as the "trust preparation of the information environment." It is the process of employing trust mechanisms to create a trusted environment to ensure our own ability to negotiate,

dictate, dominate, and move and maneuver our forces to the greatest extent possible. In order to be able to effectively manage another country's perception of a situation, a nation must first create a trust relationship, either positively or negatively, with the target country.

IO takes place at every level of war. But it is essential that trust mechanisms are employed in peacetime, in the first stage of conflict, and in the post-hostilities phase.

INFORMATION OPERATIONS RELATIONSHIPS ACROSS TIME

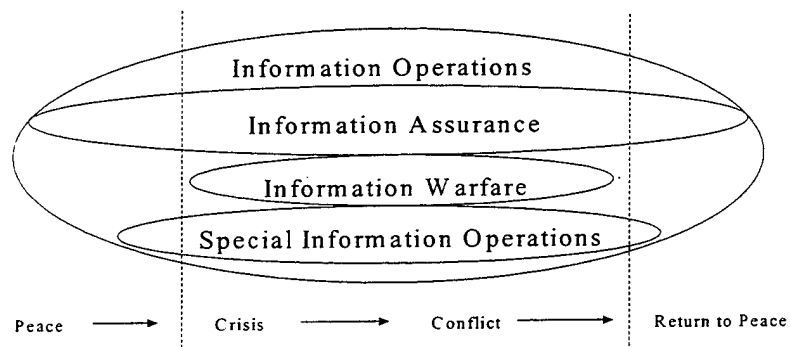


Figure 5. IO in the spectrum of conflict

E. DECEPTION

Military deception is defined in Joint doctrine as “targeting adversary decision makers through effects on their intelligence collection, analysis, and dissemination systems.” (Joint Publication 3-13) This definition is vague but the goal of a deception

operation is clear: to achieve a desired behavior from the adversary. The point then, is to build trusted relationships, for the express purpose of destroying those relationships at the properly coordinated point in time to achieve maximum combat effectiveness. This will require detailed calculations and understanding of how trust is properly modeled as well as modeling of an adversary's behavior.

The first objective though is to gain the adversary's trust. Not necessarily that they trust us at face value. They must trust the fact that they understand our actions and that those actions can be accurately predicted.

The purpose is to cause enemy commanders to form inaccurate impressions about joint or coalition force capabilities or intentions, misdirect their intelligence collection assets, or fail to employ combat or support units to their full advantage. (Joint Publication 3-13)

F. THE ECONOMY

At the strategic level and higher, much has been written about the transition from an industrial-based economy to an economy which is based on information. It is generally accepted that this transition has been taking place over the better part of the last two decades. It therefore follows that the protection of the information base is a major national security priority.

The Tofflers have described in their works the move from the Second Wave, industrial economy, to the Third Wave, information economy. (Toffler, 1980) This work

has caused many in DoD to recognize a revolution in military affairs (RMA) based on the ever-increasing power of information technology.

However, to simply recognize this dependency on information as another RMA is to fail to see the whole picture. The worldwide connectivity and instant accessibility to information does not drive the new economy, the new economy drives the need for worldwide connectivity and instant access to information; both in the military and the private sector.

PKI's will support the process by which we access global information. But the real key is trust in our economic systems. As the world continues to evolve into the "global village" (Friedman, 1999) foreseen by Thomas Friedman and others, the question will be less of competition between economies, but cooperation amongst economies so that we all can prosper.

G. PKI AND INFORMATION OPERATIONS

One of the responsibilities of the IO community is information protection. By providing a means of authentication, confidentiality, and integrity, PKI certainly supports that effort. But PKI could also be used in information operations against our forces, or in support of our forces against an adversary.

In time of crisis or war, the government could demand access to a CA and obtain access to private keys which would allow them to intercept and read electronic message traffic of adversarial governments who used that CA to obtain certificates. With the proper certificates, an intelligence organization could mount a large deception operation

either for or against the US or one of its allies. As long as the certificates were authentic, one could feed the enemy just the right amount of truthful information to appear authentic, while keeping key information secret.

H. PKI IN THE WRONG HANDS/COMPROMISE

In war casualties occur. Troops are taken prisoner. Camps are overrun. Weapons and other assets are taken by the enemy. If every soldier is carrying a smart card with PKI certificates embedded on the microchip, will those be collected by the enemy and used to his advantage if that soldier is captured? If that soldier's family receives an e-mail from him stating that he has defected to the enemy and to give away all his worldly possessions, should they believe him? Perhaps his smart card was confiscated by the enemy and they gained access to his e-mail account.

How easy is it to obtain a PKI certificate? What are the privileges of holding a PKI certificate? How quickly can the privileges of the holder of a certificate be revoked? What is the procedure for the emergency destruction of PKI material? Before we accept the PKI system in DoD and place our trust in it, procedures must be in place to account for these and other situations.

THIS PAGE INTENTIONALLY LEFT BLANK

IV. THE DISCRETIONARY-MANDATORY MODEL

A. INDUSTRIAL AGE

In the Industrial Age, the predominant form of organizational structure was an extremely disciplined, top-down hierarchy of management. The highest level of management set requirements and policies which were passed down to the lowest level worker whose purpose was to comply with those rules without question or input to the process.

Top-Down Hierarchy

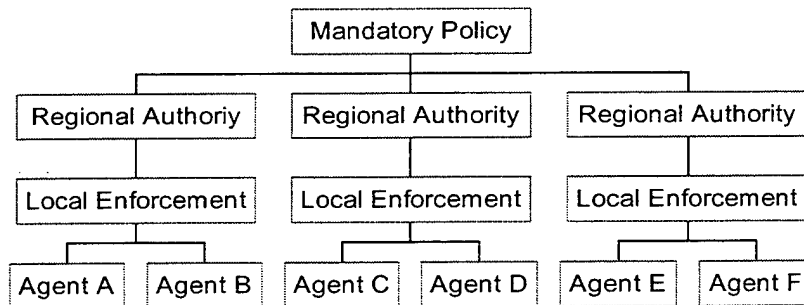


Figure 6. Top-Down Hierarchy

The most obvious application of this structure was the assembly line. Business requirements, for example, production quotas, were broken down into simplistic tasks

which assembly line workers were expected to perform without much thought process or individualistic input.

This model worked well in its time and was applied to many different organizations: corporations, militaries and governmental organizations. It has several advantages. It provides standardization, a chain-of-command, and reliability. It also has several disadvantages. It is slow, bureaucratic, and top-heavy.

However, this model does not work in today's environment. The speed at which decisions must be made today requires successful organizations to adopt a more agile structure, one that recognizes the pace at which technology and business requirements change and is complex and adaptive to those changes.

B. DISTRIBUTED MODEL

The antithesis of the hierarchial model is a purely distributed model. This model would decentralize an organization and its operations from any central authority. In effect, a purely distributed model describes a set of disconnected networks; each with its own unique characteristics.

Distributed Model

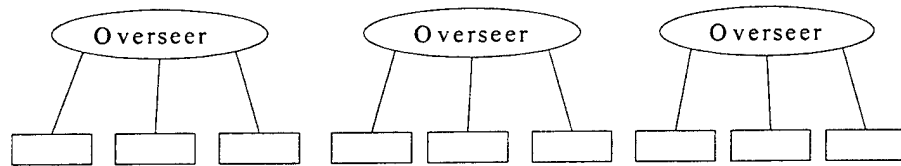


Figure 7. Distributed Architecture

The distributed model has several advantages: speed, freedom of movement, and low overhead. On the other hand, there is an entire lack of coordination among the agents. There is no standardization to support communication and trust across separated entities. Chaos is the dominant characteristic of the purely distributed model.

C. INFORMATION AGE

The reality of the Information Age is that a small group of people at the very top of an organization's management structure cannot dictate strict policies without any flexibility if they hope to survive. Much of the assembly line structure has given way to automation. Only in rare cases are the workers at the lowest levels expected to perform only mindless tasks. Today, even the lowest-level worker must be trained and trusted to make decisions which will most likely affect his organization; positively or negatively.

An example of this is today's military. The most junior member of a military unit can at any given time be put in a position where he is affecting the security policy of the United States. A private conducting border patrols in Kosovo, who makes a mistake and fires at a civilian, rather than a Serbian soldier, will quickly find himself the subject of worldwide news coverage. A pilot who fires a missile into the Chinese Embassy rather than a command and control bunker will affect foreign policy.

The speed at which information moves around the globe today has changed the way an organization must structure itself and its communications policies. The power to make decisions in an organization must be distributed throughout the organization rather than held at the very top.

D. DISCRETIONARY-MANDATORY MODEL

Neither a purely mandatory policy, nor a completely discretionary policy are sufficient when organizing to compete in today's world. A hybrid, or synergistic policy which takes the most applicable qualities of both and applies them to an organization is required.

The principles of the Discretionary-Mandatory (D-M) model are very simple. Enable those at the lowest levels the freedom of making decisions based on their own unique situations (Discretionary). At the same time the model allows the necessary direction and guidance from the upper levels of an organization in the form of mandatory policies, as well as a common set of rules and standards, which reflect the nature of the organization itself.

The D-M model is a synergistic organizational model which recognizes the value of over-arching management policies while at the same time understanding the need for distributed decision-making. The real value in the model is that it allows top-down, bottom-up and lateral flow of information and trust while allowing decisions to be made at the lowest levels possible.

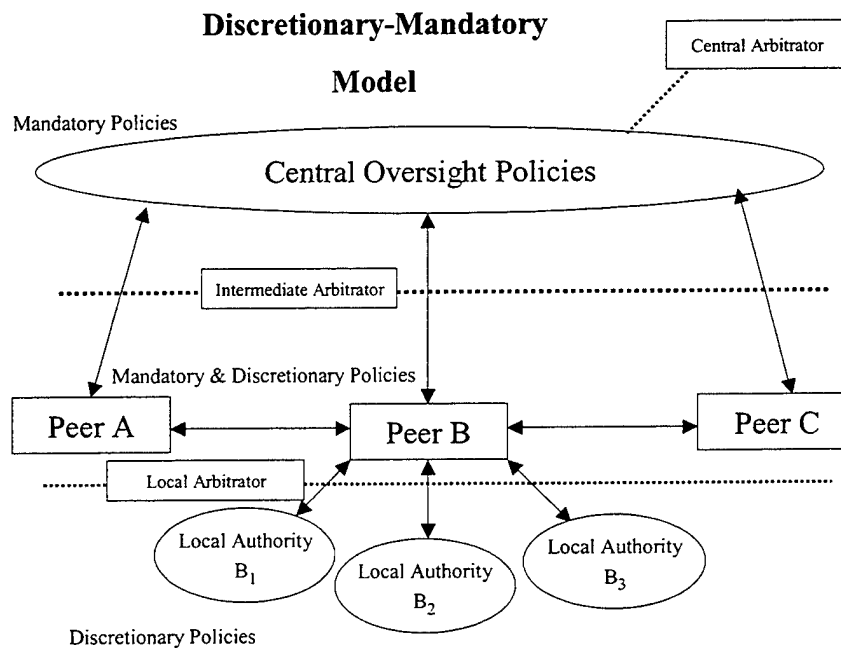


Figure 8. The Discretionary-Mandatory Model

E. MANDATORY POLICIES

Mandatory policies are those rules and requirements written by either the central oversight or by a peer organization (Figure 8). Mandatory policies should be general in scope so as to not restrict too harshly the flexibility and adaptability of the organization. No policy can be written which covers all possible situations.

In this model, the system will enforce mandatory policies. It is not left to the user to decide which policies are discretionary and which are mandatory. Much like the system of state and federal laws in the United States. Some laws apply to the entire country and some to individual states. It is not the citizen who decides which laws are relevant.

The need for mandatory policies is clear. In any organization, of any size, there should be a common set of goals and a common vision for where the organization is going. This is set by the senior leadership. One would not want the lowest level in an organization making decisions without guidance and leadership.

F. DISCRETIONARY POLICIES

Allowing subordinate levels in an organization to develop their own methods of conducting their business, within an overarching framework, provides the flexibility and adaptability essential in the Information Age. The speed at which information is transmitted and processed requires senior leadership to forego total control and allow subcomponents of their company, even to the lowest levels, the ability and trust to make decisions.

Particularly in a large organization, such as DoD, one would not want to apply the exact same requirements on a geographic Commander-in-Chief (CINC) as you would the Naval Postgraduate School (NPS). DoD has many moving parts, each with multiple diverse missions. Constricting each subcomponent into one set of policies is not the best strategy in today's fast-paced environments.

G. RULES AND PRECEDENCE

M is the set of all mandatory policies from the Central Oversight organization; the policies would form the series m_1, m_2, m_3 , etc. PM is the set of all mandatory policies promulgated by a peer level entity down to its subordinate levels. Likewise, all of these policies would form the series, pm_1, pm_2, pm_3 , etc.

PD forms the set of all discretionary policies set by a peer level entity and LD are all of the discretionary policies formed by a local entity. The policy to the left of the "is greater than" sign indicates that policy is of higher precedence and overrules the policy to the right of the sign.

In general, $m_i > mp_i$ and $m_i > pd_i$ and $m_i > ld_i$. If m_i conflicts with a higher authority, it would be considered in dispute and resolved by the central arbitrator. If a lower echelon policy conflicts with m_i , that matter will be referred to and resolved by the intermediate arbitrator. For example, the US Navy has a zero tolerance policy for narcotics use. To detect violations, random urinalysis screening is conducted at each command. When a service member tests positive for illegal drugs, his case is sent to a review board to determine the legalities of the situation. The matter becomes somewhat subjective rather than objective due to differing legal interpretations of the scientific process of drug screening. So instead of having a true zero tolerance policy, the US Navy allows each command some discretion depending on the extenuating circumstances of each case.

$MP_i > Ld_i$ and $Pd_i > Ld_i$. Similarly to the central-to-peer relationship, if MP_i or Pd_i conflicts with Ld_i , that dispute will be resolved by a local arbitrator. MP_i should not conflict with Pd_i since those policies are formed by the same entity.

H. INCORPORATING TRUST INTO THE D-M MODEL

The D-M model is not a trust model. But it is designed in a manner to facilitate trust inside and outside an organization. It does not make a trust calculation or a recommendation of trust or not to trust. What it does is realize that trust is a complex evaluation and provides the framework for giving an individual the right to trust.

Trust is a condition which when satisfied allows one party to exchange information with another party. Some trust models submit to a calculated condition of trust such as Abdul-Rahman. His model calculates trust as follows:

- For each recommendation path
 - $tv_p(T) = tv(R1)/4 \times tv(R2)/4 \times \dots \times tv(Rn)/4 \times rtv(T)$
- Merging recommendations
 - $tv(T) = \text{Average} (tv_1(T) , \dots , tv_p(T))$ (Abdul-Rahman)

In this calculation, T is the entity for which a trust value is being calculated. R1 is the recommendation trust value of the entity. For example, $tv(\text{Eric}) = tv(\text{Bob})/4 \times tv(\text{Cathy})/4 \times rtv(\text{Eric})$, where Bob and Cathy recommend Eric by supplying their trust value of Eric.

If Eric meets another entity's (Sally) trust requirements, then Sally will exchange information with Eric; otherwise they will not exchange information.

However, this assumes trust is a one-to-one relationship; that is, Sally either trusts or distrusts Eric. Trust is not a one-to-one relationship. Sally may trust Eric with some information, but not with all information. The trust relationship may change depending on the time of year, or the political or economic conditions -- nothing inherently to do with the actual trustworthiness of either party.

The act of trusting is based on a matrix of conditions as shown in Figure 9.

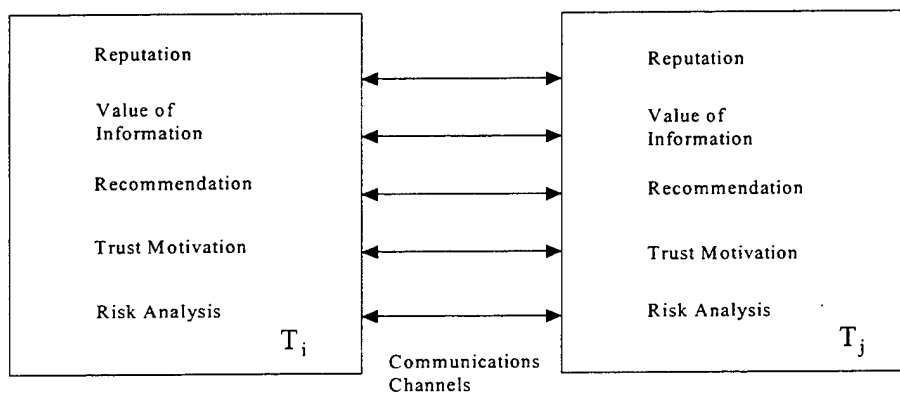


Figure 9. Trust Transaction

Figure 9 illustrates how we make trust decisions in the real world; business-to-business, business-to-government, government-to-government, etc. Trust is based not only on how "trustworthy" the receiver is, but also on the value of the information to be passed, the

potential payoffs and losses (risk analysis) for each party, the motivations of each party to trust or not to trust, as well as the historical records of each party and third party recommendations. T_i and T_j are the respective trust factors for each company's i^{th} and j^{th} pieces of information.

To illustrate, an organization such as the military distinctly classifies information into four general categories: unclassified, confidential, secret and top secret. If a military intelligence organization holds a certain piece of secret information which may be helpful to law enforcement's efforts to control narcotics, it may give that piece of information to law enforcement because they trust law enforcement not to disclose the source of that information. But if the military holds a piece of top secret and highly compartmented information, they might not give that to law enforcement personnel because they do not trust them to protect the valuable sources from which they received the information.

The D-M model reinforces trust by providing broad guidance and standardization in the form of mandatory policies, but realized the importance of flexibility and distributed decision-making in today's fast-paced environment. In the example above, mandatory policy from a high-level organization might be that anything classified top secret or above is not to be shared outside military channels. But the discretionary policy from a lower level might be to share classified information with law enforcement agencies to the greatest extent possible.

Another example of a business-to-business relationship is the recent snafu at Firestone Tire Company. Firestone has a relationship with Ford Motor Company. Ford fits many standard automobiles with Firestone products. When Firestone realized there

might be a problem with their Wilderness AT model tire, to support their reputation and trust relationship they should have passed that information to Ford. However, their motivation for sharing that information was low, because there was a high probability that Ford would publicize that information and issue a recall. Ideally, under the D-M model, Firestone would have had a mandatory policy which states: regardless of financial or economic impact, any information regarding safety will immediately be reported to the proper authorities and other corporations involved to resolve the matter. That statement would go far in instilling trust among consumers as well as potential business partners.

I. RECIPROCAL TRUST

It is obvious that a trusted system must consider ways to protect the sender from transmitting information to someone who will use it for unintended or malicious purposes. However, there also must be protection provided for the receiver. For a circuitous system to function, the receiver of information must also be able to trust the sender. The sender must be prevented from sending false, misleading, or malicious information to the receiver.

Consider the following example. A car is advertised for sale in the local newspaper classifieds. The selling price is listed as \$2500. A person arranges a meeting to inspect the car and negotiate a transaction. The car appears in good condition and all maintenance records are in order. The transaction is negotiated and the buyer writes a check for the full asking price of the car. The buyer then drives off with the car and the accompanying legal papers.

When the seller goes to the bank the next day to deposit the check, the bank reports there are insufficient funds in the buyer's account to cover the amount of the check. But the seller has already signed over legal ownership to the buyer. He is left with no car and no money from the sale.

Whenever there is trust, there is risk. But any transaction where something of value changes hands, must have support mechanisms to support trust in both directions (reciprocal trust). If the D-M model were applied to the system, there is much less risk on the part of both the buyer and the seller. The buyer and seller would agree on an intermediate arbitrator (a bank) to supervise the transaction. Based on its own local policies, the arbitrator would check each party's background against a database (e.g., criminal records, credit rating, etc.) and require a certified check to complete the transaction.

A similar situation could occur in a military setting. A spy, with sufficient documentation could pass sensitive information to a foreign military. But is the information legitimate? A strictly hierarchial process could lead a military organization down the path of deception as happened to the Russians in the Sino-Japanese War. While a purely distributed system could permit important information to slip through the cracks and be discarded.

Applying the D-M model, local policies would determine the best course of action. But it would also have to be forwarded to higher echelons to make use of the information and determine if there is a higher strategic value to the information.

V. CASE STUDY – BATTLEFIELD INFORMATION DISSEMINATION

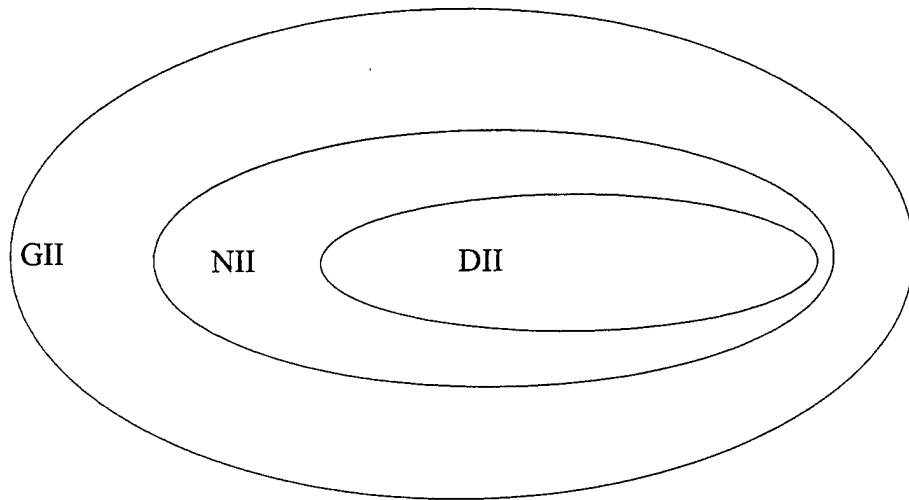


Figure 10. Information Infrastructure

A. DEFENSE INFORMATION INFRASTRUCTURE

As stated in Chapter 1, the U.S. DoD has its own information infrastructure which lies inside the larger national and global information infrastructures. It exists to support the broad dissemination of all types of information; such as tactical, operational, strategic, administrative. Physically, it consists of many types of computers, networks, and human operators.

Different types of information are transmitted in different ways. Tactical intelligence is typically gathered by some monitoring agent, forwarded to a central location to be analyzed, and then injected back into the system to be transmitted to the relevant consumers. Operational information, such as location of other naval vessels or aircraft, is broadcast to theater units from the operational command headquarters. Administrative messages are drafted, forwarded up a chain-of-command for approval and then transmitted to a list of recipients. All information is disseminated by first inputting a message into the system. The message is then projected through multiple communication paths, encrypted if necessary, to arrive at its destination.

With each step that a message takes in its chain of custody from origin to destination, the amount of trust the ultimate recipient can place in that piece of information must be decremented. The ultimate recipient will decide to act or not act based on a given piece of information. He must understand the process by which that piece of information came to him and evaluate it by asking several questions. Among these questions are the following:

- How accurate was the original piece of information?
- What was the path of the message from origination to destination?
- Could the message have been altered en route?
- What are the human factors that influence the accuracy and precision of the message and the information it contains?

Failure to evaluate the amount of trust in a given piece of data can result in tragedy, even if policy is not violated. In July 1988, the USS Vincennes shot down an Iranian jetliner because the commanding officer trusted an information system which mistakenly identified the jetliner as a hostile target; this incident resulted in a political crisis for the United States as well as adding to tensions in the Middle East. Thus, decision makers must know how to evaluate trust in information systems and be given the discretionary permissions to make their own judgments rather than following a predetermined strict decision sequence.

B. COMMAND AND CONTROL

The technology which drives Command and Control (C2) systems allows for increasing automation and speed of decision-making. However, absolute reliance on automation and Command, Control, Communications, Computers and Intelligence (C4I) systems coupled with predetermined courses of action may lead to poor decisions rather than good ones. Commanders who rely on C4I systems simply as a better way to keep track of all their tactical units are misusing valuable resources.

A better system incorporates the D-M model which allows for feedback from individual units as well as discretionary decision-making ability to be negated only by mandatory controls from higher echelons in the command structure.

C. TACTICAL INFORMATION PROCESSING

In general, tactical information is gathered, processed, and disseminated in the following process. A sensor (e.g., radar, sonar, satellite, human) gathers a piece of data;

for example, an airborne contact. The sensor sends the information to a central location to be evaluated and correlated to other information. If the data is deemed accurate, it is catalogued, identified and broadcast to all relevant organizations and other tactical units. If the data is labeled inaccurate it is dropped from the database.

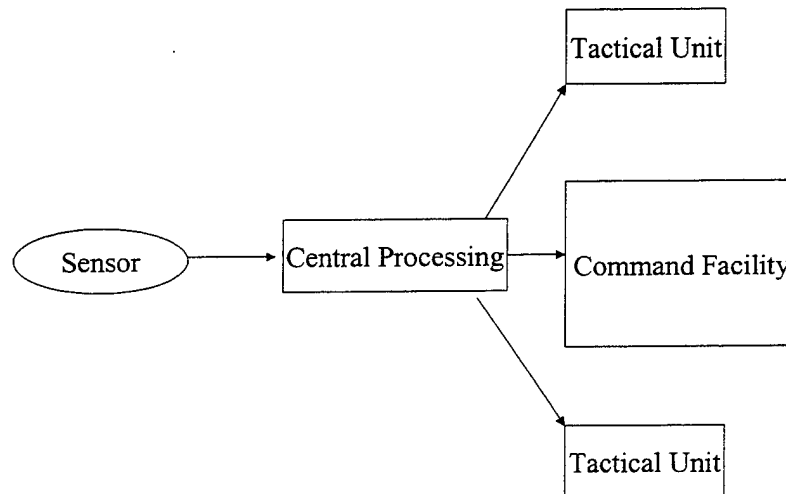


Figure 11. Tactical Information Processing

Consideration of this process raises several questions. How accurate is the initial information? How carefully was it transmitted to the initial evaluator? Was it a human being who observed the contact or an automated system? What are the flaws in the collection system?

Assuming the initial contact is accurate, the second step also brings up several questions. Who decides how to classify a contact? What are the behavior rules for other

tactical units who are in the vicinity of the contact? What information is lost between the initial contact and the central processor?

Lastly, once the data has been evaluated and is rebroadcast to other organizations, what is the possibility of tampering with the information? Could insiders, either deliberately or accidentally transmit the wrong information? Could an adversary inject false information into the system? These possibilities exploit a Top-Down organizational structure much more explicitly than one which incorporates the D-M model.

D. CASE STUDY – BATTLE GROUP CONNECTIVITY

A Carrier Battle Group (CVBG) is able to conduct sustained operations while being spread out over thousands of miles. The communications connectivity via satellite links for voice and data as well as point-to-point communications offers multiple paths across which data may be transmitted. This allows tactical and operational commanders to have access to constantly updated information about time-sensitive situations.

On the other hand, it also affords an adversary multiple opportunities to present deceptive information to our vast array of sensors in order to create confusion or give us a false sense of security. In this way an adversary could buy time, make us appear unsure of ourselves, or lead us into making a poor decision.

When a contact is acquired by a sensor, that information is transmitted to other platforms via a data link. It is also entered into a database to track over the long term. When the data on the contact is received by another platform, it appears on that platform's display in whatever symbology entered by the initial operator and classified by

the contact's type (i.e., air, surface or subsurface) as well as its relationship (i.e., friendly, unfriendly, or neutral). It is assumed that the contact was acquired, classified and retransmitted correctly.

But this is not always the case. At each point, mistakes can be made. The contact could be a decoy designed to fool our sensors. The sensor operator could be newly trained and prone to error. The data itself could have been inserted into the system by an adversary with the necessary transmitters and authentication procedures.

The extent to which one unit is allowed to trust data from another unit must be a factor. Just as important is the extent to which one unit should trust another unit with information it intends to transmit. In the Top-Down hierarchy it is not. Data is simply passed from platform to platform and, because the transmission path has been secured, it is assumed to be accurate. In the Industrial Age, when it took expensive, high-powered transmitters available only to well-financed organizations such as the military to communicate, this may have been acceptable. In the Communications Age, this assumption is no longer valid.

Consider the following scenario. An American aircraft carrier is steaming in the Persian Gulf conducting normal flight operations. It has in company an American Aegis cruiser along with a British destroyer and a Dutch frigate.

The Dutch frigate acquires a radar contact on an unknown aircraft traveling inbound which it classifies as hostile and transmits the track to the rest of the Battle Group. The frigate then loses radar contact with the aircraft but continues to update it as hostile in the Battle Group database.

The aircraft is then acquired by the Aegis cruiser at a distance of 100 kilometers from the aircraft carrier. The Aegis system determines it is the same unidentified contact classified as hostile by the Dutch frigate. It is within the air launched weapons envelope of multiple theater threat aircraft. What should the Aegis cruiser do?

Even though our own doctrine and the standing rules of engagement would likely allow the Aegis cruiser to destroy the unknown aircraft, that would make little difference in world opinion if the aircraft turned out to be an Iranian passenger jet. Alternately, if the Aegis does nothing, and the aircraft turns out to be an attack aircraft which launches its weapons on the carrier, it will have failed to carry out its duty as a naval warship.

The answer then lies in how much he trusts the information coming from the Dutch frigate. If there is an established relationship over time, common procedures and training to establish trust among the two platforms, then the cruiser can act with confidence on the data provided by the frigate. However, if there are no commonalities and no established trust relationship, then the trust factor for this individual piece of data will be low.

The Aegis platform might query the British destroyer for its data. Since the British ship is more likely to follow similar procedures, training and have similar detection systems as the American ship, their data is likely to have a higher trust factor than the Dutch warship.

Properly applied, the D-M model would account for the possible communication pitfalls in this scenario. Organizationally, the model would allow communication and procedural training to develop across platforms with no interference from a central

authority (Discretionary Policies). This process would foster a more trusted relationship amongst the platforms. The model would also force the information systems to standardize their data integrity procedures by means of central oversight policies (Mandatory Policies).

1. Information Operations

The process by which tactical information is collected, evaluated and disseminated is vulnerable to information operations attacks by an adversary. By relying on pre-planned responses and the assumption that information received is completely trustworthy, we are susceptible to deception tactics on many levels: strategic, operational and tactical.

In the scenario described above, an adversary could easily inject false information into our system, causing us to react poorly and discrediting us as a nation. If we mistakenly shoot down a civilian airliner, no one will care if we were deceived and coerced into the action.

The D-M model is the organizational model upon which Network Centric Warfare (NCW) should be based. NCW is a concept yet to be defined by our national and military leadership. But the D-M model fits the concept. It breaks the paradigm of platform centricity and allows tactical units flexibility to achieve the speed of decision-making necessary in this information-based environment. It also produces a higher level of trust in the information systems by applying standardization to each level in the model while

also recognizing that trust is not a simple one-to-one relationship, but a matrix of factors including: value of the information, risk management, and human factors.

2. Theater Engagement Plan

The scenario above also fits into a larger framework of information sharing and trust relationships. The extent to which one unit trusts another unit is important. Equally important is the extent to which we trust a potential adversary.

For example, if the unknown air contact originated from Iran, the established trust relationship between the U.S. DoD and other government agencies, would very much influence the course of action we would take in this scenario. This is precipitated by establishing communications paths through which trust relationships can begin to be constructed. The U.S. Department of State (DOS) accomplishes this through its embassies and country teams. Militarily, the geographic Commander-in-Chief (CINC) is responsible for engaging, or interacting, with the countries in his region by the establishment of the Theater Engagement Plan (TEP).

The whole point of IO is to make the correct decisions that will lead us away from conflict rather than into one. As the globalization of the world continues, avoiding conflict to conserve our own limited resources, open up new markets, and secure our own reputation throughout the world should be a national priority. The goal of the TEP should be to foster trusted relationships with the countries in each CINC's region and around the world. The more trust which can be established between countries, the more successful we will be at avoiding the tragic incidents that typically lead to war.

E. HUMAN FACTORS

What are the human factors which may affect the level of trust in this case study? Perhaps the ships have been in company before. There may be personal relationships between many of the officers and crew of each ship. Reputations may be known of the various actors in this situation. A particular commanding officer may be known for his attention to detail while another may be known for a lackadaisical approach to leadership.

All of these elements are difficult to quantify but will be factored into each decision in the process of reacting to the inbound aircraft. Would the decisions be different if the various actors could see each other face-to-face? As Rosenbloom asks, "Can trust also be established through videoteleconferencing, rapid response to chats and email, and other online media? Which of them are most likely to allow trust to develop among individuals?" (Rosenbloom, 2000)

F. INCORPORATION OF THE D-M MODEL

Applying the D-M model to this scenario, the central oversight actor would be the operational commander, in this case the numbered fleet commander. He would promulgate mandatory policies to govern the actions of units in the operational theater. The peers would be the various tactical units involved in the operations: the aircraft carrier, the Aegis cruiser, the British destroyer and the Dutch frigate. Local authorities would be the tactical action officers (TAOs) onboard the various units.

The fundamental concepts of the D-M model apply nicely to a dynamic, fast-paced and information-centric environment such as the battlefield. The model realizes the

value of the input from the lowest levels; those who are directly involved in a situation and have the greatest need for accurate and precise information.

At the same time, the model also allows for guidance, coordination and standardization from higher echelons in the organization. It also provides mechanisms for lateral communication inside an organization as well as communication across different organizations.

The D-M model is not reliant on a single input or piece of data and thus is insulated from single points of failure. It is easily applied to the short-term, single case decision-making situations. More importantly it applies to the long-term, strategic practices such as development of the TEP, foreign policy, economic policy; all of which, in their essence rely heavily on secure and trusted communications among many different countries, agencies, corporations and people.

THIS PAGE INTENTIONALLY LEFT BLANK

VI. CONCLUSION

A. SUMMARY

Conceptually, trust is important to any organization. In order to conduct business, leaders need not only to trust their own people and information systems, but also people and information systems outside their organization. U.S. DoD is no different.

In the new economy, the internet, distributed information systems, remote capabilities, all will play an important role in day-to-day affairs. The important question is how much trust can we place in these systems as face-to-face transactions become increasingly rare. As Judith and Gary Olson state in their article about trust in E-commerce, "trust needs touch". (Olson & Olson, 2000)

The U.S. DoD philosophy in designing future weapons systems and warships is to provide remote and reachback capabilities to offset decreasing manpower capabilities. A Navy ship which currently requires 400 sailors, in 2025 will require less than 100 sailors. Many requirements such as administration, medical services, intelligence services, and damage control will be remotized or be provided through reachback capabilities. For example, rather than having a doctor onboard, a technician will be provided and led step-by-step through a procedure via video-teleconference.

Reachback capabilities and remote control of operations require a shift in the trust paradigm of not only information systems but of the people involved. Who is on the other end and what is their level of expertise? What is their background? What are their true intentions and motivations? These are key questions. It is difficult to assess the intent of

others online. The inability to communicate with someone face-to-face may decrease the amount of trust we have in the overall system, depending on the situation.

B. THE D-M MODEL

The D-M model is not a computational trust model. It is a conceptual organizational model designed to better facilitate trust relationships among actors inside the organization and outside the organization. We do not claim the model to be perfect. But, in the Information Age, the concept of combining discretionary and mandatory policies to provide a synergistic effect of standardization and flexibility is important and should be applied to both newly developed organizations as well as those already established. Rather than relying simply on strict, mandatory policies, the D-M model combines the need for standard policies as well as informed consent and responsibility of individual actors to produce an effective, secure communication system.

C. TRUST RELATIONSHIPS

Trust relationships are dynamic. They are also extremely complex. They can be quantitatively modeled by assigning values to various trust factors of a particular entity such as reputation or a recommendation from a third party, and then computing an overall trust value for that entity.

But analysis suggests that a trust relationship is far more complex and requires consideration of factors which are difficult to quantify. Consider an automated information system. What level of human interaction with the system is required? What is that person's level of training with the system? How trustworthy is that individual? Is he

competent to enter accurate and precise information? What is the value of the information that is to be transferred? Answers to these questions will affect the degree to which one entity is willing to trust another at a particular point in time and for a particular type of trust relationship.

This leads to another issue. Modeling trust presents two possibilities:

- a) model trust such that the actor is an individual
- b) model trust such that the actor is composed of a group of two or more people

In order to model trust where the actor is an individual requires a great deal of granularity in representing the various objects, attributes, relationships, etc. to implement an information system. However, modeling trust where the user is a group of two or more people may tend to neglect those same objects, attributes, and relationships when computing the overall value of trust for that entity.

It is difficult to compute a simple, accurate, and precise trust factor for communication information among large organizations. The more feasible approach is to develop an organizational model, based on the D-M model, which utilizes both discretionary and mandatory policies in determining trust among entities and facilitates trust among its elements as well as between other organizations, resulting in more accurate and timely decisions being made on behalf of the organization.

D. TRUST IN THE ORGANIZATIONAL ENVIRONMENT

The U.S. DoD, along with most other organizations, must make decisions in an environment in which time is an important dimension. Each decision has short-term

(tactical), medium-term (operational), and long-term (strategic) considerations and consequences. The time frame in which information is communicated is a critical factor when deciding the trustworthiness of a piece of information. With respect to information operations (IO), timing is a challenge for the U.S. DoD: its desire for quick and easy decisions, coupled with attribution and cognitive biases, can contribute to poor decisions in the field. Additionally, failure to consider the impact of trust at each level (i.e., tactical, operational, and strategic), can lead to defeat on the battlefield.

E. INFORMATION OPERATIONS AND NETWORK CENTRIC WARFARE

Two revolutions in military affairs (RMA's) are rapidly developing in the U.S. DoD: IO and network centric warfare (NCW). Trust is a basic concept which drives the long-term elements of IO and NCW. In IO, developing long-term trusted relationships through the Theater Engagement Plan (TEP), is the key objective. In NCW, trusting information systems to give you a clear advantage in time while at the same time making accurate decisions based on the information reported from those systems is the key to a successful operation. Even in coalitions, the faster trusted relationships are developed and the degree to which the parts are interchangeable, the greater the advantage will be on the battlefield.

At the heart of any RMA is the way you organize. The D-M model is proposed as the most appropriate way for future U.S. DoD components to organize in order to maximize the advantage of time as a force multiplier.

F. FUTURE WORK

Modern information systems have created an opportunity for organizations to gather more quantitative and qualitative information for decision makers. The ability to analyze information faster and more efficiently than the competition permits organizations to better position themselves in the marketplace so as to react quickly to changes in the business environment. As organizations become more reliant on the World Wide Web (WWW), distributed information systems (e.g., multi – or federated database systems), wireless systems and virtual private networks (VPN's) to communicate and exchange information, the need of those same organizations for trust models and trust management systems will increase. Organizations will need the greater security and better authentication techniques the trust systems offer. Possible topics for further research include the following:

1. Implementation of the D-M Model into U.S. DoD Information Systems

Network centric warfare (NCW) is the concept on which future DoD operations will be carried out. This will require a paradigm shift in organizational philosophy and practice and tighter control and better security of DoD information systems. An analysis of how the D-M model would support a greater understanding of trust concepts will be needed by DoD leadership if NCW is to be successfully implemented into DoD.

2. A working D-M Trust Model

The D-M model is not a trust model. It is an organizational model which may be applied to an organization and supporting elements of an organization to facilitate trust

among the entities inside and outside of that organization. A quantifiable, working trust model would further legitimize the concepts in the D-M model for producing efficient, accurate, and timely decisions for an organization.

Many computational models already exist. Combining the conceptual ideas of the D-M model with the calculations of computational trust models developed by those such as Professor Audun Josang of Queensland University may provide interesting, workable solutions to today's security problems.

3. Quantifying the Human Factors of the D-M Model

Quantification of the human factors which affect the level of trust in a transaction would be an enormous step in developing an accurate trust model. The D-M model suggests trust relationships are complex and depend on more than just a few quantifiable factors. Human factors are perhaps the most important and complex of all the factors. If trust is to be modeled with the user as an individual person, quantifying those human elements which affect the overall trust of an organization would be extremely valuable in producing trusted systems.

Quantifying the human elements may be difficult, if not impossible. But, if they can be quantified, a more accurate trust model of individual-to-individual (i2i), business-to-business (B2B), and business-to-consumer (B2C) transactions.

4. Developing a Prototype of the D-M Model

Constructing a prototype system which incorporates the D-M model and collecting data on the effectiveness of the system as pertaining to trust and security. There

are many approaches to this concept. A honey pot system could be developed to attract users who wish to exploit the system. Deception operations could be mounted against the system to test its responsiveness. Conducting red team operations against the system to exploit possible weaknesses would provide valuable data in evaluating the effectiveness of the D-M model.

5. Apply the D-M Model to U.S. DoD Information Systems

If the future organizational structure of the U.S. DoD will be based on the concepts of NCW, the traditional organizational paradigms of DoD will need to shift from the top-down architecture to a distributed architecture. Applying the D-M model to the development of future DoD information systems and analyzing their effectiveness would add credence to the visions of NCW.

6. Apply the D-M Model to a Network Centric Warfare Organization

Applying the D-M model to a current platform-centric organization and transforming it into a network-centric organization and comparing the advantages gained by network-centricity to the disadvantages of platform-centricity will add legitimacy to the concepts of the D-M model and network centric warfare. Possible subjects of such analysis could be an aircraft carrier battle group, a special operations organization, an intelligence network, or an air wing.

7. Analyze the Model with Software

There are several software products available to model organizations and analyze their strengths and weaknesses. VITEPROJECT (VITE, 1996-1999) software simulates an organizational structure and provides statistical analysis of the effectiveness of the organization. ORGCON (EcoMerc, Inc., 1981-2000) is another product which performs similar analysis. Using these, or other software products, the D-M model could be run through several iterations of a simulation to analyze its effectiveness when applied to an actual organization.

LIST OF REFERENCES

- Abdul-Rahman, A., and Hailes, S., "A Distributed Trust Model," NSPW '97. Proceedings of the Workshop on New Security Paradigms Workshop, pp. 48-60, 1997.
- Abdul-Rahman, A., "Notes on Trust", [www-security@nsi.Rutgers.edu], 1996.
- Barton, D., "Design Issues in a Public Key Infrastructure (PKI)," [http://www.csu.edu.au/special/auugwww96/proceedings/barmoroco/barmoroco.html], 1996.
- Booker, R., "Practical PKI," *Messaging Magazine*, September/October, 1999.
- Cabletron Systems, "Public Key Infrastructure (PKI)," [http://www.Cabletron.com/vpn/VPNpki.htm], 10 June 1999.
- Cheswick, W. and Bellovin, S., *Firewalls and Internet Security*, Addison-Wesley Publishing Company, 1994.
- Chu, Y., "Trust Management for the World Wide Web," Master's Thesis, Massachusetts Institute of Technology, Boston, Massachusetts, 13 June, 1997.
- Chu, Y., Feigenbaum, J., LaMacchia, B., Resnick, P., and Strauss, M., "REFEREE: Trust Management for Web Applications," [http://www.research.att.com/~bal/papers/www6-referee/www6-referee.html], 1997.
- Comer, Douglas J., "Computer Networks and Internets", Prentice-Hall, 1999.
- Denning, Dorothy E., "Information Warfare and Security", Addison-Wesley, 2000.
- Fearnley-Sander, D., "Hermann Grassmann and the Prehistory of Universal Algebra," *American Mathematical Monthly*, v.89, pp.161-166, 1982.
- Ford, W. and Baum, M., *Secure Electronic Commerce, Building the Infrastructure for Digital Signatures and Encryption*, Prentice Hall PTR, 1997.
- EcoMerc, Inc., ORGCON organizational software, 1981-2000.
- Essin, D., "Patterns of Trust and Policy," Proceedings of the Workshop on New Security Paradigms Workshop, NSPW '97, pp. 38-47, 1997.
- Ford, W., "Public-Key Infrastructure Interoperations: Some Pragmatics," *Messaging Magazine*, September/October, 1997.

Gaines, L.T., *Trust and its Ramifications for the DoD Public Key Infrastructure*, Master's Thesis, Naval Postgraduate School, Monterey, California, September, 2000.

Gerblick, Thomas H., "IO for CINCs: Theory and Practice", U.S. Army War College, 2000.

Gerck, E., "Towards Real-World Models of Trust: Reliance on Received Information," [<http://www.mcg.org.br/trustdef.htm>], 1998.

Hansen, A., *Public Key Infrastructure (PKI) Interoperability: A Security Services Approach to Support Transfer of Trust*, Master's Thesis, Naval Postgraduate School, Monterey California, September, 1999.

Hombeck, R., "The Troubling Truth About Trust on the Internet," *EDI Dorum, The Journal of Electronic Commerce*, v. 10, no. 4, pp. 59-70, November 1998.

Josang, A. "A Logic for Uncertain Probabilities," unpublished, September 1999.

Josang, A., "A Metric for Trusted Systems," *Proceedings of the 21st National Security Conference*, NSA, 1998.

Josang, A., "A Subjective Metric of Authentication," *Proceedings of the 5th European Symposium on Research in Computer Security (ESORICS'98)*, Springer-Verlag, 1998.

Josang, A., "An Algebra for Assessing Trust in Certification Chains," *Proceedings of the Network and Distributed Systems Security (NDSS'99) Symposium*, The Internet Society, 1999.

Josang, A., "Artificial Reasoning with Subjective Logic," *Proceedings of the Second Australian Workshop on Commonsense Reasoning*, 1997.

Josang, A., "Trust-Based Decision Making for Electronic Transactions," *Proceedings of the Fourth Nordic Workshop on Secure Computer Systems (NORDSEC'99)*, Stockholm, 1999.

Josang, A., "Prospectives for Modeling Trust in Information Security," *Proceedings of the 1997 Australasian Conference on Information Security and Privacy*, Springer, 1997.

Kabay, M., *The NCSA Guide to Enterprise Security*, McGraw-Hill, 1996.

Keeney, R., *Value-Focused Thinking a Path to Creative Decision Making*, Harvard University Press, 1992.

Keeney, R., and Raiffa, H., *Decisions with Multiple Objectives*, Cambridge University Press, 1993.

Khare, R., and Rifkin, A., "Trust Management on the World Wide Web,"

[http://www.firstmonday.dk/issue3_6/khare/], June 1998.

Khare, R., and Rifkin, A., "Weaving a Web of Trust,"

Kramer, R.M., and Tyler, T.R., "Trust In Organizations – Frontiers of Theory and Research", Sage Publications 1996.

[<http://www.cs.caltech.edu/~adam/local/trust.html>], 30 November 1997.

LaMacchia, B., "The Digital Signature Trust Management Architecture,"
[<http://www.research.att.com/~bal/dsig/tma-design.htm>], 10 January 1997.

McCullagh, A., "The Establishment of 'Trust' in the Electronic Commerce Environment," [<http://www.acs.org.au/president/1998/past/io98/etrust.htm>], 7 November 1998.

Myers, A., and Liskov, B., "A Decentralized Model for Information Flow Control," *ACM SIGOPS Operating Systems Review*, v. 31, no. 5, pp. 129-142, December 1997.

Olson, J. and Olson G., "i2i Trust in E-Commerce", *Communications of the ACM*, v. 43, no. 12, pp.41-42, December 2000

Perlman, R., "An Overview of PKI Trust Models," *IEEE Network*, pp. 38-43, November/December 1999.

Pfleeger, Charles P., "Security In Computing", Prentice Hall, 1997.

"Public Key Infrastructure Roadmap for the Department of Defense," Version 2.0, Revision C, Department of Defense, May 6, 1999.

Reiter, M., and Stubblebine, S., "Authentication Metric Analysis and Design," *ACM Transactions on Information and System Security*, v. 2, no. 2, pp. 138-158, May 1999.

Render, B., and Stair, R., *Quantitative Analysis for Management*, 6th ed., Prentice Hall, 1997.

Rosenbloom, A., "Trusting Technology", *Communications of the ACM*, v. 43, no. 12, pp. 31-32, December 2000

Shelton, Henry H., "Joint Doctrine for Information Operations", Joint Chiefs of Staff, 1998.

Stallings, W., *Cryptography and Network Security Principles and Practice*, 2d ed., Prentice Hall, 1999.

Stokey, E., and Zeckhauser, R., *A Primer for Policy Analysis*, W. W. Norton and Company Inc., 1978.

Stoll, Cliff, "The Cuckoo's Egg", Simon and Schuster, 1990.

Vite, VITEPROJECT software, 1996-1999.

APPENDIX. GLOSSARY

Authentication: The process used to ascertain the identity of a subject.

Availability: Ensures that computer assets are fully operational when needed.

Back Door: An undocumented access code or procedure for accessing information.

Certificate: A data structure that securely links an entity with its corresponding public key.

Certification Authority (CA): The component of the public key infrastructure that is responsible for issuing, revoking and certifying public keys.

Certificate Revocation List (CRL): A list of certificates that have been cancelled before their expiration date.

Ciphertext: The output of an encryption algorithm, or the encrypted form of a message.

Confidentiality: Ensures that information within a computer or transmitted can only be read by authorized personnel.

Cryptography: The branch of cryptology that deals with the algorithms that encrypt and decrypt messages or files to provide security and/or authenticity. (Stallings, W., 1999)

Digital Signature: An authentication mechanism that utilizes public key cryptography to guarantee the source and integrity of a message.

Domain: The logical realm over which a CA determines policy.

Hackers: People who abuse information systems or use them to commit criminal acts.

Hash Function: A function that combines a bit string with a secret key to generate a fingerprint of the message. The recipient of the message uses the same key to generate a hash value of the message and compares the two hash values. If they are the same, the message's integrity is valid.

Integrity: Only authorized personnel can modify computer assets or transmissions.

Key: A string of bits used in encryption algorithms to encrypt plaintext and decrypt ciphertext. The string's length depends upon the type of algorithm used.

Local Registration Authority (LRA): The person or organization that is responsible to be CA for properly identifying an entity seeking a certificate.

Lightweight Directory Access Protocol (LDAP): The defacto standard for accessing directory systems.

Nonce: An identifier or number that is used with authentication techniques to combat the man-in-the-middle attack.

Non-Repudiation: A message is sent such that the identity of the sender and the integrity of the message are strong enough to prevent that party from later denying that the transaction ever occurred.

Plaintext: The message that is to be encrypted, or the message that is recovered from decryption.

Pretty Good Privacy (PGP): A public-key cryptography program that was developed primarily by Phil Zimmerman in 1991.

Private Key: One of two keys used in public key cryptography. The private key is known only to the user and should be kept secret. Only the user should have the private key. The private key decrypts the corresponding public key.

Public Key: One of two keys used in public key cryptography. The public key is made available to everyone. The public key can decrypt its corresponding private key to verify authenticity (digital signature).

Public Key Cryptography: Cryptography that uses a pair of related keys to perform cryptography. When the keys are generated, one is designated the "private key", which is kept secret and the other key is the "public key", which is available to everyone. Public key cryptography is also called asymmetric cryptography.

Public Key Infrastructure (PKI): The key management system that ensures public keys are safely, efficiently, and conveniently delivered to the system that needs them.

Registration Authority (RA): In many cases the actual identity verification is delegated from the CA to another organization called registration authority (RA).

Root Certificate Authority: The most trusted entity in a hierarchical PKI domain. It is responsible for establishing and maintaining the PKI domain. It establishes the policy, issues the certificates and delegates responsibilities to lower level CAs or LRAs. It is the trust anchor.

Subjective: The evaluation of an object or occurrence is unique to each person.

Subjective Logic: It consists of a set of algebraic operators. It can be called a calculus for uncertain probabilities.

Symmetric Cryptography: The same key that is used to encrypt the message is used to decrypt the message.

Transitivity: In the context of trust, in order for trust to be transitive in a trust path, trust must be valid for each member in the path. For example, Bob trusts Sue, and Sue trusts Tom, transitivity assumes that Bob trust Tom.

Trojan Horse: An innocent looking program that has additional malicious functions.

Trust Anchor: The CA that is fully trusted by a user. This means that the user has complete trust in the CA's public key.

Trust Models: They attempt to automate the logic, variables, and thought processes that a human performs when making a trust decision.

Trusted Path: The verification path that a user must take to verify a certificate with a trusted CA.

Virus: A self- replicating computer program. A virus is often malicious code embedded in an executable program.

Worm: A self-replicating program, but unlike a virus it does not need a host to propagate, it is designed to spread on its own. It is malicious in that it performs a denial of service attack.

X.509 Standard: The standard that defines the structure and functionality for certificates and CRLs.

THIS PAGE INTENTIONALLY LEFT BLANK

INITIAL DISTRIBUTION LIST

1. Defense Technical Information Center2
8725 John J. Kingman Road, Ste 0944
Fort Belvoir, VA 22060-6218

2. Dudley Knox Library2
Naval Postgraduate School
411 Dyer Road
Monterey, CA 93943-5101

3. Dean Dan Boger1
Code CC/BO
Naval Postgraduate School
Monterey, CA 93943-5118

4. Professor James Bret Michael, Code CS/Mj1
Naval Postgraduate School
Monterey, CA 93943-5118

5. Mr. Terry Mayfield1
Computer and Software Engineering Division
Institute for Defense Analysis
1801 North Beauregard Street
Alexandria, VA 22311-1772

6. Professor John McHugh1
SEI/CERT
4500 5th Avenue
Room 4420
Pittsburgh, PA 15213-3890

7. Professor Audun Josang1
DSTC Pty Ltd
Level 7, GP South (Bldg 78)
The University of Queensland
Brisbane, QLD 4072
Australia

8. Professor Carl R. Jones1
Code IS/JS
Naval Postgraduate School
Monterey, CA 93943-5118

9. Lieutenant Daniel R. Hestad1
Naval Postgraduate School
Code 32 – Information Systems & Operations
2 Monterey Circle
Monterey, CA 93943